现代数学基础丛书 159

算法数论

（第二版）

裴定一　祝跃飞　编著

科学出版社

现代数学基础丛书 159

算 法 数 论

(第二版)

裴定一　祝跃飞　编著

科 学 出 版 社

北 京

内 容 简 介

本书论述了算法数论的基本内容, 其中涉及同余式、二次剩余、特征、连分数、代数数域、椭圆曲线、素性检验、大整数因子分解算法、椭圆曲线上的离散对象、超椭圆曲线、格理论等分支, 也介绍了这些知识在密码学中的一些应用. 本书的特点是内容涉及面广, 在有限的篇幅内, 包含了必要的预备知识和数学证明, 尽可能形成一个比较完整的体系. 本书的部分内容曾多次在中国科学院研究生院信息安全国家重点实验室和广州大学作为硕士研究生教材使用.

本书可作为信息安全、数论等专业的研究生教材, 以及相关专业的研究人员、高等学校的教师和高年级学生的参考书.

图书在版编目(CIP)数据

算法数论/裴定一, 祝跃飞编著. —2 版. —北京: 科学出版社, 2015.7
(现代数学基础丛书; 159)

ISBN 978-7-03-045332-7

Ⅰ. ①算… Ⅱ. ①裴… ②祝… Ⅲ. ①算法理论 Ⅳ. ①O241

中国版本图书馆 CIP 数据核字(2015) 第 186575 号

责任编辑: 李静科 / 责任校对: 张凤琴
责任印制: 徐晓晨 / 封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

北京教图印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2002 年 9 月第 一 版 开本: 720×1000 1/16
2015 年 9 月第 二 版 印张: 15 1/2
2015 年 9 月第一次印刷 字数: 293 000

定价: 78.00 元

(如有印装质量问题, 我社负责调换)

《现代数学基础丛书》编委会

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言, 书籍与期刊起着特殊重要的作用. 许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍, 从中汲取营养, 获得教益.

20世纪70年代后期, 我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了 10 余年, 而在这期间国际上数学研究却在迅猛地发展着. 1978 年以后, 我国青年学子重新获得了学习、钻研与深造的机会. 当时他们的参考书籍大多还是50年代甚至更早期的著述. 据此, 科学出版社陆续推出了多套数学丛书, 其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出, 前者出版约40卷, 后者则逾80卷. 它们质量甚高, 影响颇大, 对我国数学研究、交流与人才培养发挥了显著效用.

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者, 针对一些重要的数学领域与研究方向, 作较系统的介绍. 既注意该领域的基础知识, 又反映其新发展, 力求深入浅出, 简明扼要, 注重创新.

近年来, 数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用, 还形成了一些交叉学科. 我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域.

这套丛书得到了许多数学家长期的大力支持, 编辑人员也为其付出了艰辛的劳动. 它获得了广大读者的喜爱. 我们诚挚地希望大家更加关心与支持它的发展, 使它越办越好, 为我国数学研究与教育水平的进一步提高做出贡献.

杨　乐

2003 年 8 月

第二版前言

本书的第一版于 2002 年 9 月出版, 目的是介绍与公钥密码相关的数论算法. 近年来, 公钥密码有了很多新的发展, 本版新增以下内容.

1. 二次剩余和格理论是数论中两个古老的分支, 近年来在密码理论中得到了重要应用. 第二版在第一版基础上增添了这两方面的内容. 3.4 节介绍二次剩余假设的概念. 基于二次剩余假设这一数学难题, 8.5 节构造了一个概率公钥密码, 并证明它具有多项式安全.

2. 格密码是密码学界研究的热点问题之一, 第 13 章 “格” 是第一版附录中的 A.5 节的扩充. 本章介绍格的基本理论及其在密码学中的应用, 包括格的基本概念和 LLL 算法, 以及 LLL 算法在背包问题求解和小指数 RSA 密码算法分析中的应用, 最后介绍两类基于格中数学难题设计的公钥密码体制, 包括 NTRU 密码体制和基于 LWE 难题的全同态加密体制.

此外, 第二版中还增加了 “名词索引”.

作　者

2015 年 4 月

第一版前言

算法数论是一门对数论问题进行算法设计和算法分析的学科. 它的历史可以追溯到古希腊 Eratosthenes 氏筛法构造素数表. 但它真正成为一门学科, 是在 20 世纪中叶, 一方面是由于计算机科学的发展和计算复杂度理论的建立为算法数论奠定了理论基础; 另一方面是数论发展的内部推动力, 如对数论中某些问题 (如一些猜想) 给出肯定与否的回答的过程中, 收集依据时涉及一些大数据量的实例的验证, 而这已经超出了人们的手算能力, 只能借助计算机编程来完成; 更重要的是由于一些基于数论的公钥密码方案的提出和对其攻击所涉及的一些数论问题求解算法的发现.

公钥密码是在 20 世纪 70 年代中期提出的一类新型的密码, 它尤其适合在计算机网络环境下使用, 具有加密信息、管理密钥和数字签名等功能, 能保证信息的机密性、完整性和不可否认性. 迄今为止所提出的公钥密码, 其安全性都建立在某个数学难题的基础之上, 所谓 “数学难题”, 确切地说是求解这个数学问题, 目前还没有多项式时间的算法被发现. 例如, 大整数因子分解、有限域或椭圆曲线离散对数等问题. 只要选择适当的参数, 在现有的技术条件下, 这些问题都是很难解决的, 这就为相应的公钥密码的安全性奠定了基础. 在解决这些难题方面所取得的任何重大进展, 都会对相应的公钥密码的使用产生巨大的影响.

RSA 公钥密码、ElGamal 公钥密码和椭圆曲线公钥密码是目前影响最大的三类公钥密码. 前者是在 20 世纪 70 年代中叶提出来的, 它的安全性依赖于大整数因子分解的难度, 后两者的安全性分别依赖于计算有限域离散对数和椭圆曲线离散对数的难度. 椭圆曲线公钥密码是 20 世纪 80 年代中叶提出来的, 由于其自身具有一些其他公钥体制无法比拟的优势, 近十年来已成为公钥密码研究的一个十分活跃的方向, 研究所获得的许多有关的椭圆曲线的算法, 大大丰富了算法数论的理论.

因子分解和离散对数是算法数论研究的两个核心问题. 本书的主要内容是介绍这两个问题的基本理论, 以及迄今为止所提出的主要算法的基本原理. 这部分内容包含在第 9~11 章. 第 9 章介绍 Miller-Rabin 概率型素性检验方法, 以及分别利用特征和、椭圆曲线的确定型检验方法. 第 10 章重点介绍椭圆曲线因子分解方法及数域筛法. 第 11 章包含有关有限域及椭圆曲线上的离散对数的主要结果. 其余各章 (除第 8 章) 都是为这最后三章作准备的. 第 1~5 章介绍初等数论的有关知识, 第 6 章介绍代数数论的有关预备知识, 第 7 章介绍椭圆曲线的有关预备知识. 第 8 章介绍前五章的初等数论知识在密码学中的一些应用. 为了本书的系统性, 添加一个附录, 介绍一些代数和有限域的一些算法.

本书的选材是经过精心考虑的, 内容涉及面很广, 但在有限的篇幅内, 包含了必要的预备知识和数学证明, 尽可能形成一个较完整的体系. 考虑到信息安全专业的研究生有来自数学本科和非数学本科两类, 在利用本书时, 可以根据需要, 选择不同的章节组成一个学期的教学. 对于来自数学本科的学生, 前五章可以较快地通过, 而把重点放在后面几章. 对于来自非数学本科的学生, 第 7~11 章有关代数数论和椭圆曲线的章节可以考虑不讲. 本书的部分内容曾多次在中国科学院研究生院信息安全国家重点实验室和广州大学作为硕士研究生教材.

本书的编写和出版得到国家自然科学基金跨学科重点项目 “电子商务系统中的信息安全理论和技术的研究” (批准号 19931010), 国家 973 项目 “信息与网络安全体系结构” (批准号 G1999035804) 和 “中国科学院研究生教材基金” 的资助, 特此感谢.

作　者

2001 年 4 月

目　录

第 1 章　整数的因子分解

1.1　唯一分解定理

数论是研究自然数 $1, 2, 3, \cdots$ 性质的一门数学分支. 自然数是人们日常生活中用得最多的一类数. 历史上, 人们很早就开始研究数论, 它已成为内容十分丰富的一个分支. 数论在信息安全、计算机科学、数字信号处理等现代科技领域有重要的应用, 所以, 数论至今仍是一门充满活力、蓬勃发展的分支.

通常, 用 $\mathbb{Z}$ 表示整数集合, 整数即为

$$0, \quad \pm 1, \quad \pm 2, \cdots .$$

自然数就是正整数.

定理 1.1　设 a 和 b 为整数, $b>0$, 则存在整数 q 和 r, 使

$$a = qb + r, \quad 0 \leqslant r < b,$$

r 称为 b 除 a 所得的最小正剩余.

证明　以 $\left[\frac{a}{b}\right]$ 表示不超过分数 $\frac{a}{b}$ 的最大整数, 则

$$0 \leqslant a - \left[\frac{a}{b}\right] b < b,$$

取 $q = \left[\frac{a}{b}\right], r = a - \left[\frac{a}{b}\right] b$, 即证得定理.

当 b 除 a 的最小正剩余 r 为零时, 称 b 为 a 的因子, a 为 b 的倍数, 记为 $b|a$.

若 b 为 a 的因子, $b \neq 1, b \neq a$, 这时称 b 为 a 的真因子, 显然有 $0 < |b| < |a|$, 这里 $|a|$ 为 a 的绝对值.

若 $b \neq 0,\ c \neq 0$, 显然有：

(1) 若 $b|a,\ c|b$, 则 $c|a$;

(2) 若 $b|a$, 则 $bc|ac$;

(3) 若 $c|d,\ c|e$, 则对任意 m, n 有 $c|dm+en$.

自然数 $p(\neq 1)$, 若仅以 1 和自身 p 为其因子, 称 p 为素数. 非素数的自然数 $n\ (\neq 1)$ 称为复合数.

设 M 为整数的一个子集合, 如果它对加、减法封闭, 即若 $m,n \in M$, 则 $m \pm n \in M$, 这时称 M 为模. a 为任一整数, a 的所有的倍数就组成一个模. 相反的结论也成立, 即如下定理.

定理 1.2　任一非零模, 必为一正整数的诸倍数组成的集合.

证明　设 d 为该模中最小正整数, 则模中其他数必为 d 之倍数. 若不然, 设 n 为模中 d 之非倍数, 由定理 1.1, 存在整数 q 及 r, 使

$$n = qd + r, \quad 0 < r < d.$$

由于 $r = n - qd$ 也属于此模, 这与 d 为该模中最小正整数的假设相矛盾, 故模中其他各数都为 d 的倍数. 因为 d 在模中, 所以 d 的任一倍数也在模中. 定理即证.

命 a,b 为二整数, 集合

$$\{ma + nb \mid m,n \in \mathbb{Z}\}$$

即为一模, 此模中最小正整数 d 称为 a,b 的最大公因子, 记为 $d = (a,b)$.

由定理 1.2 的证明, 不难证得下述定理.

定理 1.3　(a,b) 具有下述性质:

(1) 有整数 x,y, 使 $(a,b) = ax + by$;

(2) 对任二整数 x,y, 必有 $(a,b)|ax + by$;

(3) 若 $c|a$, $c|b$, 则 $c|(a,b)$.

由于 (3), 也称 (a,b) 为 a,b 的最大公因子.

定理 1.4　设 p 为素数且 $p|ab$, 则 $p|a$ 或 $p|b$.

证明　若 $p \nmid a$, 则 $(a,p) = 1$, 由定理 1.3 知有二整数 x,y, 使

$$ax + py = 1,$$

所以

$$abx + pyb = b.$$

由 $p|ab$ 可知 $p|b$, 证毕.

定理 1.5(唯一分解定理)　任一自然数 n 皆可唯一地表为素数之积

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. \tag{1.1}$$

这里, $p_1 < p_2 < \cdots < p_k$ 为素数, $a_1, a_2, \cdots, a_k$ 为自然数.

证明　首先证明 n 可以表为素数之积, 然后再证明上述表法唯一.

若 n 为素数, 定理显然成立. 当 n 不是素数时, 设 p_1 是 n 的最小的真因子, 则 p_1 一定是素数, 因 p_1 的真因子也是 n 的真因子, 所以 p_1 不能有真因子. 设

$n = p_1 n_1 \ (1 < n_1 < n)$, 对 n_1 重复上述推理, 得 $n = p_1 p_2 n_2$, p_2 为素数, $1 < n_2 < n_1$, 继续执行此法, 得 $n > n_1 > n_2 > \cdots > 1$, 此做法最多不能超过 n 次, 最后必得

$$n = p_1 p_2 \cdots p_l,$$

也可排为式 (1.1) 中的形式.

今设

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

为 n 的两个分解式, 其中 $p_1 < p_2 < \cdots < p_k$, $q_1 < q_2 < \cdots < q_l$ 都为素数, 利用定理 1.4, 任一 p_i 必为某一 q_j, 任一 q_i 也必为某一 p_j, 故 $k = l, p_i = q_i \ (1 \leqslant i \leqslant k)$, 又若 $a_1 > b_1$, 则

$$p_1^{a_1 - b_1} p_2^{a_2} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{b_k},$$

左边为 p_1 的倍数, 右边不是 p_1 的倍数, 这是不可能的, 同样 $a_1 < b_1$ 也不可能, 故 $a_1 = b_1$. 类似地, 可证得 $a_i = b_i \ (i = 1, 2, \cdots, k)$, 唯一性得证.

给定一自然数 n, 当它很大时, 例如, 一百多位的十进制数, 要将它因子分解, 实非易事. 在第 10 章将讨论一些大整数因子分解的算法, 随之而来的一个问题是如何判断一个数是否是素数, 在第 9 章将讨论几个素性判断的方法.

1.2　辗转相除法 (欧氏除法)

若 a, b 为二自然数, $a \geqslant b$, 以 (a, b) 表示 a 和 b 的最大公因子. 由定理 1.3 知, 有二整数 x, y, 使

$$(a, b) = ax + by.$$

如何计算 (a, b), 又如何找到上述 x 和 y, 定理 1.1 实际上已经给出了所要的算法.

首先用 b 除 a 得到商 q_0, 余数 r_0, 即

$$a = q_0 b + r_0, \quad 0 \leqslant r_0 < b. \tag{1.2}$$

如果 $r_0 = 0$, 那么 b 是 a 的因子, a, b 的最大公因子就是 b. 如果 $r_0 \neq 0$, 用 r_0 除 b 得到商 q_1, 余数 r_1, 即

$$b = q_1 r_0 + r_1, \quad 0 \leqslant r_1 < r_0. \tag{1.3}$$

如果 $r_1 = 0$, 那么 r_0 除尽 b, 由式 (1.2) 知, r_0 也除尽 a, r_0 是 a, b 的公因子. 反之, 任何一个除尽 a, b 的数, 由式 (1.2) 知, 也除尽 r_0, 因此 r_0 是 a, b 的最大公因子. 如果 $r_1 \neq 0$, 则用 r_1 除 r_0 得到商 q_2, 余数 r_2，即

$$r_0 = q_2 r_1 + r_2, \quad 0 \leqslant r_2 < r_1. \tag{1.4}$$

如果 $r_2 = 0$, 那么由式 (1.3) 可知, r_1 是 r_0, b 的公因子, 由式 (1.2) 知, r_1 也是 a, b 的公因子. 反之, 如果一整数除得尽 a, b, 那么由式 (1.2) 知, 它一定除得尽 r_0 , 由式 (1.3) 知, 它一定除得尽 r_1, 所以 r_1 是 a, b 的最大公因子.

若 $r_2 \neq 0$, 再用 r_2 除 r_1, 重复上述过程, 依次得到 $b > r_0 > r_1 > r_2 > \cdots$, 逐步小下来, 而又都非负. 经过有限步后, 一定会有某个 r 为零. 若设 r_n 是第一个出现的零, 则 r_{n-1} 就是 a, b 的最大公因子. 所得到的一串算式为

$$
\begin{aligned}
&a = q_0 b + r_0, \\
&b = q_1 r_0 + r_1, \\
&r_0 = q_2 r_1 + r_2, \\
&r_1 = q_3 r_2 + r_3, \\
&\qquad \cdots\cdots \\
&r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, \\
&r_{n-2} = q_n r_{n-1}.
\end{aligned}
$$

由第一式可得

$$
r_0 = a - q_0 b,
$$

由第二式可得

$$
r_1 = b - q_1 r_0 = -q_1 a + (1 + q_0 q_1) b,
$$

一般地, 对任一 r_i $(0 \leqslant i \leqslant n-1)$, 都有二整数 x_i, y_i, 使

$$
r_i = x_i a + y_i b.
$$

由于

$$
\begin{aligned}
r_i &= r_{i-2} - q_i r_{i-1} \\
&= (x_{i-2} a + y_{i-2} b) - q_i (x_{i-1} a + y_{i-1} b) \\
&= (x_{i-2} - q_i x_{i-1}) a + (y_{i-2} - q_i y_{i-1}) b,
\end{aligned}
$$

所以有递推公式

$$
\begin{aligned}
&x_0 = 1, \qquad && x_1 = -q_1, \qquad && x_i = x_{i-2} - q_i x_{i-1}, \\
&y_0 = -q_0, && y_1 = 1 + q_0 q_1, && y_i = y_{i-2} - q_i y_{i-1}.
\end{aligned}
$$

这样, 可以找到二整数 x, y, 使

$$
(a, b) = ax + by.
$$

看一个例子：求 4862 和 2156 的最大公因子, 则有

$$\begin{aligned}&4682 = 2 \times 2156 + 550,\\&2156 = 3 \times 550 + 506,\\&550 = 506 + 44,\\&506 = 11 \times 44 + 22,\\&44 = 2 \times 22.\end{aligned}$$

可见 $(4862, 2156) = 22$, 利用上述算式可得

$$\begin{aligned}&550 = 4862 - 2 \times 2156,\\&506 = -3 \times 4862 + 7 \times 2156,\\&44 = 4 \times 4862 - 9 \times 2156,\\&22 = -47 \times 4862 + 106 \times 2156.\end{aligned}$$

称上述求 a, b 的最大公因子的算法为辗转相除法, 或欧几里得除法.

考虑辗转相除法所需的比特计算量. 仍设 $a \geqslant b$, 若 a 和 b 用二进制表示的长度分别为 k 和 l, 则 $k \leqslant \log_2 a + 1$, $l \leqslant \log_2 b + 1$. 用 b 除 a 得到商和余数, 这个带余除法所需的比特计算量为 $O(kl)$(这里 $O(kl)$ 表示一个 $\leqslant c \cdot kl$ 的量, 其中 c 为一个不依赖 k 和 l 的常数), 也可表为 $O(\lg^2 a)$. 还需要知道带余除法要做多少次.

我们有 $r_{j+2} < \dfrac{1}{2} r_j$.

首先来证明这个论断. 若 $r_{j+1} \leqslant \dfrac{1}{2} r_j$, 则 $r_{j+2} < r_{j+1} \leqslant \dfrac{1}{2} r_j$, 即证. 若 $r_{j+1} > \dfrac{1}{2} r_j$, 则 $r_j = r_{j+1} + r_{j+2}$, 同样有 $r_{j+2} < \dfrac{1}{2} r_j$.

以上论断表示, 做两次带余除法可将余数缩小一半. 要得到 (a, b), 所要做的带余除法的次数不会超过 $2[\log_2 a] = O(\lg a)$, 因而辗转相除法所需的比特计算量为

$$O(\lg^2 a) \times O(\lg a) = O(\lg^3 a).$$

给定自然数 a, b, 若已知它们的因子分解

$$\begin{aligned}&a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i \geqslant 0 \quad (1 \leqslant i \leqslant s);\\&b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \quad \beta_i \geqslant 0 \quad (1 \leqslant i \leqslant s),\end{aligned}$$

则

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}.$$

若以 $[a, b]$ 表示 a, b 的最小公倍数 (即 $[a, b]$ 是 a 和 b 的倍数, 且任一 a 和 b 的公倍数都是 $[a, b]$ 的倍数), 则

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_s^{\max(\alpha_s, \beta_s)}.$$

易见

$$(a,b)[a,b]=a\cdot b.$$

对于多个自然数 $a_1,a_2,\cdots,a_k$, 也可以定义它们的最大公因子和最小公倍数.

1.3 Mersenne 素数和 Fermat 素数

n 为一自然数, 以 $\sigma(n)$ 表示 n 的所有因子之和.

定理 1.6 若 $n=p_1^{a_1}\cdots p_s^{a_s}$, 则

$$\sigma(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\ \cdots\ \frac{p_s^{a_s+1}-1}{p_s-1}.$$

证明 n 的因子都形如

$$p_1^{x_1}\cdots p_s^{x_s},\quad 0\leqslant x_1\leqslant a_1,\cdots,\quad 0\leqslant x_s\leqslant a_s,$$

故

$$\begin{aligned}\sigma(n)&=\sum_{x_1=0}^{a_1}\cdots\sum_{x_s=0}^{a_s}p_1^{x_1}\cdots p_s^{x_s}\\&=\sum_{x_1=0}^{a_1}p_1^{x_1}\cdots\sum_{x_s=0}^{a_s}p_s^{x_s}\\&=\frac{p_1^{a_1+1}-1}{p_1-1}\ \cdots\ \frac{p_s^{a_s+1}-1}{p_s-1}.\end{aligned}$$

定义 1.1 若 n 的所有因子之和等于 $2n$, 即 $\sigma(n)=2n$, 则 n 称为完全数.

例 1.1 $\sigma(6)=1+2+3+6=2\times 6,\quad \sigma(28)=1+2+4+7+14+28=2\times 28.$

定理 1.7 若 $p=2^n-1$ 为素数, 则

$$\frac{1}{2}p(p+1)=2^{n-1}(2^n-1)$$

为偶完全数, 且无其他偶完全数存在.

证明 由定理 1.6 知

$$\sigma\left(\frac{1}{2}p(p+1)\right)=\frac{2^n-1}{2-1}\frac{p^2-1}{p-1}=p(p+1),$$

故 $2^{n-1}(2^n-1)$ 为完全数.

若 a 为一偶完全数, 令

$$a=2^{n-1}u,\quad n>1,\quad 2\nmid u,$$

则

$$2^n u = 2a = \sigma(a) = \frac{2^n - 1}{2 - 1} \cdot \sigma(u),$$

故

$$\sigma(u) = \frac{2^n u}{2^n - 1} = u + \frac{u}{2^n - 1},$$

可知 $2^n - 1|u$, u 和 $\frac{u}{2^n - 1}$ 都是 u 的因子, 但 $\sigma(u)$ 是 u 的所有因子之和, 故 u 只有两个因子, 即 u 为素数, 且

$$\frac{u}{2^n - 1} = 1,$$

所以 $a = 2^{n-1}(2^n - 1)$, 证毕.

是否有奇完全数存在, 这是至今尚未解决的数论难题. 偶完全数的问题化为形如 $2^n - 1$ 的素数的问题.

定理 1.8 若 $n > 1$, 且 $a^n - 1$ 为素数, 则 $a = 2$, n 为素数.

证明 若 $a > 2$, 则 $(a-1)|a^n - 1$, 故 $a^n - 1$ 非素数.

若 $a = 2$, 而 $n = kl$, 则 $(2^k - 1)|2^n - 1$, 故 $a^n - 1$ 非素数. 证毕.

整数 $M_n = 2^n - 1$ 称为第 n 个 Mersenne 数, 当 p 为素数, $M_p = 2^p - 1$ 为素数时, M_p 称为 Mersenne 素数. 至今已知道有 29 个 Mersenne 素数, 所对应的 29 个 p 为

2	3	5	7	13	17	19	31	61	89
107	127	521	607	1279	2203	2281	3217	4253	4423
9689	9941	11213	19937	21701	23209	44497	86243	132049	

第 25 和 26 个 Mersenne 素数 M_{21701} 和 M_{23209} 分别是在 1978 和 1979 年由中学生发现的, 第 29 个 Mersenne 素数 M_{132049} 是在 1983 年找到的, 它有 39751 位. 至今尚不知道是否有无穷个 Mersenne 素数存在.

定理 1.9 若 $2^m + 1$ 为素数, 则 $m = 2^n$.

证明 若 m 有一个奇因子 q, 命 $m = qr$, 则

$$2^{qr} + 1 = (2^r)^q + 1 = (2^r + 1)(2^{r(q-1)} - \cdots + 1),$$

而 $1 < 2^r + 1 < 2^{qr} + 1$, 故 $2^m + 1$ 非素数, 证毕.

命 $F_n = 2^{2^n} + 1$, 称为 Fermat 数, 最前五个 Fermat 数

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

都是素数, 据此, Fermat 猜测凡 F_n 皆为素数, 但 Euler 在 1732 年举出

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417,$$

故 Fermat 猜想并不正确, 现已证明

$$n = 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73,$$

F_n 皆非素数. 因此有人推测仅存在有限个 Fermat 素数.

1990 年几百名研究人员利用联网的一千多台计算机, 运行了六个星期, 将 F_9 分解为 7 位、49 位、99 位三个素数之积, F_9 有 155 位, 此项成果被列为 1990 年世界十大科技成果之一.

1.4 整系数多项式

以 $\mathbb{Q}$ 表示全体有理数$\left\{\dfrac{a}{b}\middle| a, b \in \mathbb{Z}, b \neq 0\right\}$集合, $\mathbb{Q}[x]$ 表示全体有理系数多项式集合. $\mathbb{Q}[x]$ 与 $\mathbb{Z}$ 有很多相似的性质. $\mathbb{Q}[x]$ 对加法、减法、乘法是封闭的, 关于除法, 类似于定理 1.1, 有如下结论.

定理 1.10　设 $f(x), g(x) \in \mathbb{Q}[x]$, 则有 $q(x), r(x) \in \mathbb{Q}[x]$ 使

$$f(x) = q(x)g(x) + r(x),$$

$r(x) = 0$ 或 $r(x) \neq 0$, 且 $\deg r(x) < \deg g(x)$.

当 $r(x) = 0$ 时, 称 $g(x)$ 能除尽 $f(x)$, 记为 $g(x)|f(x)$, $g(x)$ 称为 $f(x)$ 的因子.

设 M 为 $\mathbb{Q}[x]$ 中一子集, 若它具有下述性质:

(1) 若 $f(x), g(x) \in M$, 则 $f(x) - g(x) \in M$;

(2) 若 $f(x) \in M$, 对任一 $q(x) \in \mathbb{Q}[x]$, 有 $q(x)f(x) \in M$,

则称 M 为一理想.

$\mathbb{Q}[x]$ 中任一多项式 $f(x)$ 与 $\mathbb{Q}[x]$ 中所有多项式的乘积组成的集合是一个理想, 称为主理想, 以 (f) 表示. 反之, 类似于定理 1.2, 则有如下定理.

定理 1.11　$\mathbb{Q}[x]$ 中任一理想都是主理想.

证明　设 $M \subset \mathbb{Q}[x]$ 为一理想, $d(x)$ 为 M 中次数最低的多项式. 若 M 中有一多项式 $g(x)$, $d(x)$ 不是 $g(x)$ 的因子, 则由定理 1.10 知, 有二多项式 $q(x), r(x) \neq 0$, 使得

$$g(x) = q(x)d(x) + r(x), \quad \deg r(x) < \deg d(x).$$

由于 $r(x) = g(x) - q(x)d(x)$, 所以 $r(x) \in M$, 这与 $d(x)$ 是 M 中次数最低的多项式矛盾, 故 $M = (d)$, 定理成立.

定理 1.11 的证明与定理 1.2 的证明是完全类似的, $\mathbb{Q}[x]$ 中多项式次数起了 $\mathbb{Z}$ 中的绝对值的作用.

利用定理 1.10 也可有辗转相除法计算两个多项式的最大公因子.

类似于定理 1.5, 也可证明 $\mathbb{Q}[x]$ 上有唯一因子分解定理. $\mathbb{Q}[x]$ 中的不可约多项式类似于 $\mathbb{Z}$ 中的素数. $p(x)$ 称为不可约多项式, 若 $q(x)|p(x)$, 则 $q(x)$ 为常数或为 $p(x)$ 乘一常数.

考虑整系数多项式的因子分解.

定理 1.12　命 $g(x)$ 及 $h(x)$ 为二整系数多项式

$$\begin{aligned} g(x) &= a_l x^l + \cdots + a_0, \quad & a_l \neq 0, \\ h(x) &= b_m x^m + \cdots + b_0, \quad & b_m \neq 0, \end{aligned}$$

以及

$$g(x)h(x) = c_{l+m}x^{l+m} + \cdots + c_0,$$

则

$$(a_l, \cdots, a_0)(b_m, \cdots, b_0) = (c_{l+m}, \cdots, c_0).$$

证明　不失一般性, 可假定 $(a_l, \cdots, a_0) = 1, (b_m, \cdots, b_0) = 1$, 若考虑素数 $p|(c_{l+m}, \cdots, c_0)$ 及

$$\begin{aligned} &p|(a_l, \cdots, a_{\mu+1}), \quad p \nmid a_\mu, \\ &p|(b_m, \cdots, b_{v+1}), \quad p \nmid b_v, \end{aligned}$$

由定义可得

$$c_{\mu+v} = \sum_{s+t=\mu+v} a_s b_t,$$

其中除 $a_\mu b_v$ 一项, 皆为 p 之倍数. 因 $p \nmid a_\mu b_v$, 故 $p \nmid c_{\mu+v}$, 因此 $p \nmid (c_{l+m}, \cdots, c_0)$, 与假设矛盾, 故 $(c_{l+m}, \cdots, c_0) = 1$, 证毕.

定理 1.13(Gauss)　命 $f(x)$ 为一整系数多项式, 若

$$f(x) = g(x)h(x),$$

这里 $g(x), h(x)$ 为二有理系数多项式, 则有一有理数 r, 使

$$r \cdot g(x), \quad \frac{1}{r}h(x)$$

都为整系数多项式.

证明　可假定 $f(x)$ 的系数的最大公因子是 1, 有二整数 M 及 N 使

$$\begin{aligned} Mg(x) &= a_l x^l + \cdots + a_0, \quad a_i \text{ 为整数}, \\ Nh(x) &= b_m x^m + \cdots + b_0, \quad b_i \text{ 为整数}, \\ MNf(x) &= c_{l+m}x^{l+m} + \cdots + c_0. \end{aligned}$$

由假定及定理 1.12, 可知

$$MN = (c_{l+m}, \cdots, c_0) = (a_l, \cdots, a_0) \cdot (b_m, \cdots, b_0).$$

令

$$r = \frac{M}{(a_l, \cdots, a_0)} = \frac{(b_m, \cdots, b_0)}{N},$$

则 $r \cdot g(x)$ 和 $\dfrac{1}{r}h(x)$ 皆有整系数, 证毕.

定理 1.13 是说, 整系数多项式在有理数域上可分解当且仅当在整数环上可分解.

定理 1.14(Eisenstein)　命

$$f(x) = c_n x^n + \cdots + c_0$$

为一整系数多项式, 若 $p \nmid c_n$, $p | c_i$ $(0 \leqslant i < n)$, 且 $p^2 \nmid c_0$, 则 $f(x)$ 不可约.

证明　假定 $f(x)$ 可约, 由定理 1.13 可知,

$$f(x) = g(x)h(x),$$

$$g(x) = a_l x^l + \cdots + a_0, \quad h(x) = b_m x^m + \cdots + b_0, \quad l + m = n, \quad l > 0, \quad m > 0,$$

a_i 和 b_k 均为整数, 由 $c_0 = a_0 b_0$ 及 $p | c_0$ 可知, $p | a_0$ 或 $p | b_0$. 设 $p | a_0$, 则由 $p^2 \nmid a_0 b_0 = c_0$ 可得 $p \nmid b_0$.

又 $g(x)$ 的系数不能都为 p 之倍数, 因若不然, 则 $p | c_n$, 故可假定

$$p | (a_0, \cdots, a_{r-1}), \quad p \nmid a_r, \quad 1 \leqslant r < l,$$

由

$$c_r = a_r b_0 + \cdots + a_0 b_r$$

可知 $p \nmid c_r$, 因 $r \leqslant l < n$, 与假定矛盾.

由定理 1.14 可得:

(1) $x^n - p$ 在 $\mathbb{Z}$ 上不可约;

(2) $\dfrac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1$ 在 $\mathbb{Z}$ 上不可约.

证明　命 $x = y + 1$, 则 (2) 变为

$$\frac{1}{y}\big((y+1)^p - 1\big) = y^{p-1} + p y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + p,$$

除第一个系数, 其他系数都是 p 的倍数, 而常数项不是 p^2 的倍数.

1.5 环 $\mathbb{Z}[i]$ 和 $\mathbb{Z}[\omega]$

设 R 为一个环, 若存在 R 的非零元素集合到集合 $\{0,1,2,\cdots\}$ 的一个映射 λ, 它具有下述性质: 对任意 $a,b\in R$, $b\neq 0$, 存在 $c,d\in R$, 使 $a=cb+d$, d 或为零, 或 $\lambda(d)<\lambda(b)$, 称 R 为欧氏环.

整数环 $\mathbb{Z}$ 是欧氏环, 其上的绝对值就可作为 λ 函数. 多项式环 $\mathbb{Q}[x]$ 也是欧氏环, 多项式的次数可作为 λ 函数.

定理 1.15 欧氏环 R 中任一理想都是主理想.

证明 设 M 为 R 的一个理想, 考虑非负整数集合 $\{\lambda(b)|b\in M, b\neq 0\}$, 它一定有一个最小数, 即存在 $a\in M$, 使 $\lambda(a)\leqslant\lambda(b)$, $b\in M$, 可以证明 $M=R\cdot a$. 因对任一 $b\in M$, 存在 $c,d\in R$, 使 $b=ca+d$, d 或为零, 或有 $\lambda(d)<\lambda(a)$. 由于 $d=b-ca\in M$, 所以不能有 $\lambda(d)<\lambda(a)$, 因而一定有 $d=0$, 则 $b\in R\cdot a$, 证毕.

可以证明, 在任一主理想环中, 唯一因子分解定理都成立.

再给出两个欧氏环的例子.

令 $\mathrm{i}^2=-1$, 定义 $\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}|a,b\in\mathbb{Z}\}$. $\mathbb{Z}[\mathrm{i}]$ 在加法、减法和乘法之下是封闭的, 成为一个环, 在 $\mathbb{Z}[\mathrm{i}]$ 上定义函数 λ: $\lambda(a+b\mathrm{i})=a^2+b^2$, 易见,

$$\lambda(a+b\mathrm{i})=(a+b\mathrm{i})(a-b\mathrm{i}),\quad \lambda\big((a+b\mathrm{i})(c+d\mathrm{i})\big)=\lambda(a+b\mathrm{i})\lambda(c+d\mathrm{i}).$$

设 $\alpha=a+b\mathrm{i}$, $\gamma=c+d\mathrm{i}\neq 0$, 则

$$\frac{\alpha}{\gamma}=\frac{(a+b\mathrm{i})(c-d\mathrm{i})}{c^2+d^2}=r+s\mathrm{i},$$

r,s 为有理数, 取 $m,n\in\mathbb{Z}$, 使 $|r-m|\leqslant 1/2$, $|s-n|\leqslant 1/2$, 令 $\delta=m+n\mathrm{i},\rho=\alpha-\delta\gamma$, 则若 $\rho\neq 0$ 时, 有

$$\begin{aligned}\lambda(\rho)&=\lambda(\alpha-\delta\gamma)=\lambda(\gamma(\alpha/\gamma-\delta))\\&=\lambda(\gamma)\cdot\lambda(\alpha/\gamma-\delta)=\lambda(\gamma)((r-m)^2+(s-n)^2)\\&\leqslant(1/4+1/4)\lambda(\gamma)<\lambda(\gamma),\end{aligned}$$

由此可见, $\mathbb{Z}[\mathrm{i}]$ 成为一欧氏环.

令 $\omega=\dfrac{-1+\sqrt{-3}}{2}$, ω 为三次本原根, 即 ω 是方程 $x^2+x+1=0$ 的根, 定义 $\mathbb{Z}[\omega]=\{a+b\omega|a,b\in\mathbb{Z}\}$, $\mathbb{Z}[\omega]$ 成为一个环, 在 $\mathbb{Z}[\omega]$ 上引进函数 λ:

$$\lambda(a+b\omega)=(a+b\omega)(a+b\omega^2)=a^2+b^2+ab(\omega+\omega^2)=a^2-ab+b^2,$$

亦有 $\lambda(\alpha)=\alpha\overline{\alpha}$.

设 $\alpha,\beta\in\mathbb{Z}[\omega]$, $\beta\neq 0$, 则 $\dfrac{\alpha}{\beta}=\dfrac{\alpha\overline{\beta}}{\beta\overline{\beta}}=r+s\omega,r,s$ 为有理数, 取 $m,n\in\mathbb{Z}$, 使 $|r-m|\leqslant 1/2,|s-n|\leqslant 1/2$, 令 $r=m+n\omega$, 则

$$\lambda\left(\frac{\alpha}{\beta}-\gamma\right)=(r-m)^2-(r-m)(s-n)+(s-n)^2\leqslant\frac{1}{4}+\frac{1}{4}+\frac{1}{4}<1.$$

因而取 $\rho=\alpha-\gamma\beta$, 则 $\rho=0$, 或 $\lambda(\rho)=\lambda(\beta)\lambda\left(\dfrac{\alpha}{\beta}-\gamma\right)<\lambda(\beta)$. 可见 $\mathbb{Z}[\omega]$ 是欧氏环.

习　　题

习题 1.1　设 $(u,v)=1$, 试证: $(u+v,u-v)=1$或2.

习题 1.2　n 为任一自然数, 试证: $30|n^5-n$ 及 $42|n^7-n$.

习题 1.3　以 $\mathrm{ord}_p a$ 表示 a 的因子分解式中所含 p 的幂次. 试证:
$\mathrm{ord}_p(a+b)\geqslant\min(\mathrm{ord}_p a,\mathrm{ord}_p b)$, 且当 $\mathrm{ord}_p a\neq\mathrm{ord}_p b$ 时, 等号成立.

习题 1.4　证明以下各数不是有理数:

$$\log_{10}2,\quad \sqrt{2},\quad \sqrt[n]{m}(m\text{不是一个整数的 } n \text{ 次幂}).$$

习题 1.5　假定素数只有有限个, 记为 $p_1,p_2,\cdots,p_n$, 证明: $p_1p_2\cdots p_n+1$ 是素数, 因此素数有无穷多个.

习题 1.6　设 $n>2$, 证明在 n 和 $n!$ 之间一定有一个素数, 由此也能推出素数有无穷多个.

习题 1.7　设 $n\geqslant 0$, $F_n=2^{2^n}+1$, 再设 $m\neq n$. 证明: 若 $d>1$, 且 $d|F_n$, 则 $d\nmid F_m$. 由此推出素数有无穷多个.

习题 1.8　设整系数多项式 $P(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$, $a_0\neq 0$. 证明: 若 $P(x)$ 有有理根 x_0, 则 x_0 必是整数, 且 $x_0|a_0$.

习题 1.9　证明所有形如 $2^p-1(p$ 为素数) 的 Mersenne 整数都是两两互素的.

习题 1.10　设 a 和 b 为整数, $a>b$, $(a,b)=1$. 证明:

$$(a^m-b^m,a^n-b^n)=a^{(m,n)}-b^{(m,n)}.$$

习题 1.11　证明下列多项式在整数环上不可分解:

$$x^2+1,\quad x^4+1,\quad x^6+x^3+1.$$

习题 1.12　定义 $\mathbb{Z}[\sqrt{-2}]=\{a+b\sqrt{-2}|a,b\in\mathbb{Z}\}$, 试证 $\mathbb{Z}[\sqrt{-2}]$ 成一环. 在 $\mathbb{Z}[\sqrt{-2}]$ 上引入函数: $\lambda(a+b\sqrt{-2})=a^2+2b^2$, 利用 λ 试证 $\mathbb{Z}[\sqrt{-2}]$ 成一欧氏环.

习题 1.13　设 p 是素数, 如果 $p^\lambda \leqslant n < p^{\lambda+1}$, 证明

$$\mathrm{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^\lambda}\right]$$

习题 1.14　证明 $Z[\mathrm{i}]$ 中的元素 α 是可逆元当且仅当 $\alpha \cdot \bar{\alpha} = 1$, 由此推出 $Z[\mathrm{i}]$ 中的可逆元有且仅有 $\pm 1, \pm \mathrm{i}$.

习题 1.15　证明在环 $Z[\mathrm{i}]$ 中, $1 + \mathrm{i}$ 是不可约元, 试求 2 的分解式.

习题 1.16　证明 $Z[\omega]$ 中的元素 α 是可逆元当且仅当 $\alpha \cdot \bar{\alpha} = 1$, 由此推出 $Z[\omega]$ 中的可逆元有且仅有 $\pm 1, \pm\omega, \pm\omega^2$.

习题 1.17　证明在 $Z[\omega]$ 中, 3 被 $(1-\omega)^2$ 整除, 试求 3 的分解式.

习题 1.18　用欧几里得辗转相除法, 求 $(2108, 3720, 2046)$.

第 2 章　同　余　式

2.1　孙 子 定 理

我国古代的一部优秀数学著作《孙子算经》中, 有 “物不知其数” 一问:

“今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何”.

这个问题的意思可以表达如下: 譬如, 有一把围棋子, 三个三个地数, 最后余下两个, 五个五个地数, 最后余下三个, 七个七个地数, 最后余下两个, 问这把棋子有多少个?

在程大位著的《算法统宗》(1593 年) 中, 可以用四句诗给出上述问题的解法:

三人同行七十稀,　五树梅花廿一枝,
七子团圆正月半,　除百零五便得知.

它的意思是说, 所求之数除以 3 所得的余数乘 70, 除以 5 所得的余数乘 21, 除以 7 所得的余数乘 15, 然后总加起来, 如果它大于 105, 则减去 105, 还大再减去, 最后得出的正整数就是答数了.

所以以上孙子算经上的问题的解答, 可以这样来算:

$$2 \times 70 + 3 \times 21 + 2 \times 15 = 233,$$

减去两个 105, 得 23, 这就是答数了.

为什么 70, 21 和 15 有此妙用? 先来看看 70, 21, 15 的性质, 70 是这样一个整数: 用 3 除余 1, 用 5 与 7 都除得尽, 所以 $70a$ 是 3 除余 a, 5 与 7 除得尽的数; 21 是 5 除余 1, 3 与 7 除得尽的数, 所以 $21b$ 是 5 除余 b, 而 3 与 7 除得尽的数. 同样地, $15c$ 是 7 除余 c, 而 5 与 3 除得尽的数. 总起来正整数

$$70a + 21b + 15c$$

是 3 除余 a, 5 除余 b, 7 除余 c 的数, 也就是可能的解答数, 但不一定是最小的, 该数加减 105 仍然有同样性质, 因 105 是 3, 5, 7 的最小公倍数, 所以可以多次减去 105 得出最小的正整数解答来.

以上算法称为孙子定理, 在国外文献上也称为中国剩余定理, 这个方法不但在古代数学史上占有地位, 而且这个算法的原则在近代数学上还常被采用. 在以上的

问题中, 遇到的是 3 除, 5 除, 7 除, 如果用别的数代替 3, 5, 7, 能否有同样类似的解法? 这里就要研究同余式的理论了.

设 n 为自然数, a, b 为任意两个整数, 若 $a-b$ 能被 n 除尽, 则称 a 与 b 模 n 同余, 记为

$$a \equiv b(\bmod n).$$

换句话说, 这时 n 除 a 所得的余数与 n 除 b 所得的余数相同.

用同余式表示 "物不知其数" 问题, 就是要求一个 (最小的) 正整数 x, 使

$$\begin{cases} x \equiv 2 \,(\bmod 3), \\ x \equiv 3 \,(\bmod 5), \\ x \equiv 2 \,(\bmod 7). \end{cases}$$

这是一个解同余方程组的问题. 关于这一类同余方程组, 有如下的定理.

定理 2.1 命 m 为 m_1, m_2 的最小公倍数, 同余方程组

$$x \equiv a_1 \,(\bmod m_1), \tag{2.1}$$

$$x \equiv a_2 \,(\bmod m_2) \tag{2.2}$$

有解的充分必要条件是 $(m_1, m_2) | a_1 - a_2$, 如果这条件成立, 则方程组有且仅有一个小于 m 的非负整数解.

证明 (1) 命 $(m_1, m_2) = c$, 由式 (2.1) 与式 (2.2) 立得

$$x \equiv a_1 \,(\bmod c), \quad x \equiv a_2 \,(\bmod c),$$

故 $a_1 - a_2 \equiv 0 \,(\bmod c)$, 因此如果式 (2.1), 式 (2.2) 有公共解, 则 $c | a_1 - a_2$.

(2) 反之, 若 $c | a_1 - a_2$, 由式 (2.1) 得

$$x = a_1 + m_1 y, \tag{2.3}$$

代入式 (2.2) 得

$$a_1 + m_1 y = a_2 + m_2 z,$$

即

$$\frac{a_1 - a_2}{c} = \frac{m_2}{c} z - \frac{m_1}{c} y. \tag{2.4}$$

由于 $(m_1/c, m_2/c) = 1$, 利用辗转相除法, 可以找到整数 p, q, 使

$$\frac{m_2}{c} p - \frac{m_1}{c} q = 1.$$

取 $z = p \cdot (a_1 - a_2)/c,\ y = q(a_1 - a_2)/c$, 式 (2.4) 就有解, 式 (2.1) 与式 (2.2) 也就有公解 $a_1 + m_1 y = a_2 + m_2 z$.

(3) 如果式 (2.1), 式 (2.2) 有两个解, 即除 x, 还有 x', 则

$$x - x' \equiv 0 \pmod{m_1}, \quad x - x' \equiv 0 \pmod{m_2},$$

所以 $m|x - x'$, 因而在 0 与 $m - 1$ 之间有且仅有一个 x 适合式 (2.1), 式 (2.2), 定理证毕.

对于两个整数 m, n, 如果 m 与 n 的最大公因子 $(m, n) = 1$, 则称 m 与 n 互素. 当 m_1 与 m_2 互素时, 定理 2.1 的条件肯定满足, 这时式 (2.1), 式 (2.2) 一定有解. 利用数学归纳法, 可以把这个结果推广到更一般的情况: 设 $m_1, m_2, \cdots, m_k$ 两两互素, 则下面同余方程组

$$\begin{gathered} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \cdots\cdots \\ x \equiv a_k \pmod{m_k} \end{gathered}$$

在 $0 \leqslant x < M = m_1 m_2 \cdots m_k$ 内有唯一的解. 记 $M_i = M/m_i\ (1 \leqslant i \leqslant k)$, 因 $(M_i, m_i) = 1$, 故有二整数 p_i, q_i, 使

$$M_i p_i + m_i q_i = 1.$$

记 $e_i = M_i p_i$, 可见

$$e_i \equiv 0 \pmod{m_j}\ (j \neq i), \quad e_i \equiv 1 \pmod{m_i},$$

所以

$$e_1 a_1 + e_2 a_2 + \cdots + e_k a_k$$

是上述同余方程组的解, 加减 M 的倍数后, 就可得到最小非负整数解.

2.2 剩 余 类 环

定理 2.2 (1) $a \equiv a \pmod{m}$ (反身性);

(2) 若 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$ (对称性);

(3) 若 $a \equiv b \pmod{m}, b \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$ (传递性).

称具有以上三条性质的关系为等价关系.

以上三条性质, 将整数分成了 m 个类, 每一类由互相同余的数组成, m 个类分别对应余数为 $0, 1, 2, \cdots, m - 1$, 任两个类不能有公共元, 称这些类为剩余类.

定理 2.3 若

$$a \equiv a_1, \quad b \equiv b_1 \pmod{m},$$

则 $a+b \equiv a_1+b_1, a-b \equiv a_1-b_1, ab \equiv a_1b_1 \pmod{m}$.

证明很容易, 以最后一式为例:

$$m|a(b-b_1)+b_1(a-a_1)=ab-a_1b_1.$$

上述定理也可改述如下: 任给二剩余类 A, B, 其中各取一代表元 a 和 b, 命 $a+b$(或 $a-b, ab$) 所代表的类为 C, 则 C 仅与 A, B 有关, 而与所取的代表元无关. 可将 C 表为 $A+B$(或 $A-B, AB$). 可见剩余类所成的集合可以定义加法、减法和乘法, 但一般地说, 没有除法, 如 $3 \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{4}$, 但 $3 \not\equiv 1 \pmod{4}$.

定理 2.4 若

$$ac \equiv bd, \quad c \equiv d \pmod{m}$$

及 $(c, m)=1$, 则 $a \equiv b \pmod{m}$.

证明 由

$$(a-b)c+b(c-d)=ac-bd \equiv 0 \pmod{m}$$

可得

$$m|(a-b)c,$$

但 $(m, c)=1$, 故得 $m|a-b$, 证毕.

以 O 表示 m 的倍数组成的类, 易知

$$A+O=A, \quad A \cdot O=O.$$

以 I 表示以 m 除余 1 的数组成的类, 易见

$$A \cdot I=A,$$

但由

$$A \cdot B=A \cdot C$$

不一定能得到 $B=C$, 当 A 中的数与 m 互素 (A 中若有一个数与 m 互素, 则其余各数都与 m 互素) 时, 就可得到 $B=C$.

模 m 的 m 个剩余类组成一个环, 记为 $\mathbb{Z}/(m)$, 当 $m=p$ 为素数时, $\mathbb{Z}/(p)$ 对加减乘除都封闭 (做除法时, 不能用 O 去除), 成为一个域, 它含 p 个元素.

当 n 与 m 互素时, 存在二整数 x, y, 使

$$nx+my=1.$$

这时, $nx \equiv 1 \pmod{m}$, n 所在的剩余类在 $\mathbb{Z}/(m)$ 中有逆元素 x. 在模 m 的各剩余类中取一代表元 $a_1, a_2, \cdots, a_m$, 称为 m 的一个完全剩余系.

下面给出一个应用剩余类的例子.

有 N 个运动队参加一个单循环比赛, 每个队与其余 $N-1$ 个队都要比赛一次. 现在要安排比赛程序表. 当 N 为奇数时, 增添一个虚设的队, 在每一轮中, 与虚设队比赛的队为轮空, 所以不妨假设 N 为偶数.

将 N 个队依次编号为 $1, 2, 3, \cdots, N$, 共需进行 $N-1$ 轮比赛. 在第 k 轮 $(1 \leqslant k \leqslant N-1)$, 若 $1 \leqslant i, j \leqslant N-1, i \neq j, i+j \equiv k \pmod{N-1}$, 则第 i 队与第 j 队比赛. 第 N 队则与由 $2i^* \equiv k \pmod{N-1}$ 所决定的第 i^* 队比赛. 由于 $N-1$ 为奇数, 2 与 $N-1$ 互素, 存在整数 q, 使 $2q \equiv 1 \pmod{N-1}$, 故 $i^* \equiv kq \pmod{N-1}$ 唯一决定.

按上述方法编排的比赛程序, 在 $N-1$ 轮比赛中每个队与其余各队都比赛一次. 设 $1 \leqslant i \leqslant N-1$, 第 i 队在第 k_N 轮与第 N 队比赛, 这里 $k_N \equiv 2i \pmod{N-1}$ 唯一决定, 与第 j 队 $(j \neq i, 1 \leqslant j \leqslant N-1)$ 在第 k_j 轮比赛, 这里 $k_j \equiv i+j \pmod{N-1}$ 也唯一决定, 所以第 i 队与各队都比赛一次, 前 $N-1$ 队在 $N-1$ 轮中与第 N 队各比赛一次, 当然第 N 队与各队也都比赛一次.

例如, 若有 5 个队参加单循环赛, 添加一个虚设的队, 故取 $N=6$, 按上述方法可排出下列比赛程序:

队别 / 第 n 轮	1	2	3	4	5
第 1 轮	5	4	×	2	1
第 2 轮	×	5	4	3	2
第 3 轮	2	1	5	×	3
第 4 轮	3	×	1	5	4
第 5 轮	4	3	2	1	×

2.3　Euler 函数 $\varphi(m)$

在模 m 的一个剩余类中, 若有一个数与 m 互素, 则该剩余类中所有数都与 m 互素. 这时称该剩余类与 m 互素.

与 m 互素的剩余类个数记为 $\varphi(m)$, $\varphi(m)$ 称为 Euler(欧拉) 函数. $\varphi(m)$ 也就是 $1, 2, \cdots, m-1$ 中与 m 互素的数的个数. 在与 m 互素的 $\varphi(m)$ 个剩余类中各取一个代表元

$$a_1, \quad a_2, \cdots, \quad a_{\varphi(m)},$$

它们组成一个缩剩余系, 简称为缩系.

定理 2.5(Euler 定理) 若 $(k,m)=1$, 则

$$k^{\varphi(m)} \equiv 1 \,(\text{mod } m).$$

证明 设 $a_1, a_2, \cdots, a_{\varphi(m)}$ 为一缩系, 由于 $(k,m)=1$, 则

$$ka_1, \quad ka_2, \cdots, \quad ka_{\varphi(m)} \tag{2.5}$$

中各数也都与 m 互素, 且其中任二数模 m 都不同余. 否则, 若 $ka_i \equiv ka_j \,(\text{mod } m)$, 由于 $(k,m)=1$, 将有 $a_i \equiv a_j \,(\text{mod } m)$. 所以式 (2.5) 中各数也组成一个缩系, 于是

$$\prod_{i=1}^{\varphi(m)} (ka_i) \equiv \prod_{i=1}^{\varphi(m)} a_i \,(\text{mod } m).$$

由于 $(a_i, m)=1$, 易知 $k^{\varphi(m)} \equiv 1 \,(\text{mod } m)$, 证毕.

当 p 为素数时, 易知 $\varphi(p)=p-1$, 更进一步, 对素数幂 p^n, 有

$$\varphi(p^n) = p^n - p^{n-1} = p^n(p-1).$$

定理 2.6(Fermat 小定理) 若 p 为素数, 则对所有整数 a 有同余式

$$a^p \equiv a \,(\text{mod } p).$$

证明 由定理 2.5 及 $\varphi(p)=p-1$, 立得.

设 m 为任一复合数, 如何计算 $\varphi(m)$?

定理 2.7 若 $(m,m')=1$, x 过 m 之一完全剩余系, x' 过 m' 之一完全剩余系, 则 $mx'+m'x$ 过 mm' 之一完全剩余系.

证明 在 mm' 个数 $mx'+m'x$ 中, 若

$$mx'+m'x \equiv my'+m'y \,(\text{mod } mm'),$$

则

$$mx' \equiv my' \,(\text{mod } m'), \quad m'x \equiv m'y \,(\text{mod } m).$$

由于 $(m,m')=1$, 可得

$$x' \equiv y' \,(\text{mod } m'), \quad x \equiv y \,(\text{mod } m),$$

定理证毕.

定理 2.8 若 $(m,m')=1$, x 过 m 之一缩系, x' 过 m' 之一缩系, 则 $mx'+m'x$ 过 mm' 之一缩剩余系.

证明　(1) $mx'+m'x$ 与 mm' 互素, 否则, 必有一素数 p, 使 $p|(mx'+m'x, mm')$, 假定 $p|m$, 则 $p|m'x$, 因 $(m,m')=1$, 故 $p\nmid m'$, 即 $p|x$, $p|(m,x)$, 这不可能.

(2) 凡与 mm' 互素之数 a 必与一形如

$$mx'+m'x,\quad (x,m)=1,\quad (x',m')=1$$

之数模 mm' 同余. 由定理 2.7, 有二整数 x,x' 使

$$a\equiv mx'+m'x (\mathrm{mod}\ mm'),$$

今证 $(m,x)=1, (m',x')=1$, 若 $(x,m)=d\neq 1$, 则

$$(a,m)=(mx'+m'x,m)=(m'x,m)=(x,m)=d\neq 1,$$

与原假定相背, 同法可证 $(x',m')=1$.

(3) 在定理 2.7 中已证在形如 $mx'+m'x$ 之数中无同余者, 故得定理.

由定理 2.8 立得如下定理.

定理 2.9　若 $(m,m')=1$, 则

$$\varphi(mm')=\varphi(m)\varphi(m'),$$

即 $\varphi(m)$ 为一积性函数.

定理 2.10　若 $m=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}, p_1<p_2<\cdots<p_s$, 则

$$\varphi(m)=m\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right).$$

证明　设 $m=p_1^{l_1}\cdots p_s^{l_s}, p_1<p_2<\cdots<p_s$, 由定理 2.9 可得

$$\varphi(m)=\prod_{i=1}^{s}\varphi(p_i^{l_i})=\prod_{i=1}^{s}(p_i^{l_i}-p_i^{l_1-1})=m\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right).$$

2.4　同 余 方 程

考虑一次不定方程

$$ax+by=n$$

的整数解 x,y.

定理 2.11　方程 $ax+by=n$ 有整数解的充分必要条件是 $(a,b)|n$.

证明 若该方程有解, 显然有 $(a,b)|n$, 反之, 设 $(a,b)|n$, 有二整数 x_0, y_0, 使 $ax_0 + by_0 = (a,b)$, 则

$$a\frac{x_0 n}{(a,b)} + b\frac{y_0 n}{(a,b)} = n,$$

即证.

定理 2.12 若 $(a,b)=1$, 且 x_0, y_0 为 $ax+by=n$ 的一解(此解的存在无问题), 则该方程任一解可表为

$$x = x_0 + bt, \quad y = y_0 - at,$$

且对任何整数 t, 此皆为解.

证明 由

$$ax + by = n \quad 及 \quad ax_0 + by_0 = n$$

可得

$$a(x-x_0) + b(y-y_0) = 0.$$

因 $(a,b)=1$, 故 $a|(y-y_0)$, 命 $y = y_0 - at$, 则 $x = x_0 + bt$. 反之, 对任意 t, 此两式显然是解.

今讨论形如

$$ax + b \equiv 0 \pmod{m} \tag{2.6}$$

的同余方程, 何时有解? 有多少个模 m 的剩余类适合此方程?

解方程 (2.6), 即为求方程

$$ax + b = my$$

的整数解. 利用定理 2.11 可得如下结果.

若 $(a,m)=1$, 则有 x_0, y_0, 使

$$ax_0 + my_0 = 1,$$

故 $x = -bx_0$ 即为式 (2.6) 之解. 这时式 (2.6) 的解是唯一的 (在模 m 的意义下), 因若有两个解 x, x', 则

$$ax + b \equiv 0 \pmod{m}, \quad ax' + b \equiv 0 \pmod{m},$$

故

$$a(x - x') \equiv 0 \pmod{m}.$$

由于 $(a,m)=1$, 故 $m|x-x'$, 仅有模 m 的一个剩余类适合式 (2.6).

若 $(a,m)=d>1$, 则 $d|b$, 否则无解, 如此得

$$\frac{a}{d}x+\frac{b}{d}\equiv\frac{m}{d}y\left(\mathrm{mod}\frac{m}{d}\right),\quad \left(\frac{a}{d},\frac{m}{d}\right)=1. \tag{2.7}$$

由上述证明, 已知式 (2.7) 必有唯一解 x_1 适合 $0\leqslant x_1<\frac{m}{d}$, 而

$$x=x_1+\frac{m}{d}t$$

皆为式 (2.7) 之解, 故对模 m 有

$$x_1,\quad x_1+\frac{m}{d},\quad x_1+2\cdot\frac{m}{d},\cdots,\quad x_1+(d-1)\frac{m}{d}$$

皆不同余, 均为式 (2.6) 之解, 故得如下结论.

定理 2.13　若 $(a,m)|b$, 则式(2.6)有 (a,m) 个模 m 互不同余的解, 不然无解.

定理 2.14　同余方程

$$a_1x_1+\cdots+a_nx_n+b\equiv 0\,(\mathrm{mod}\ m)$$

有解 $(x_1,\cdots,x_n)$ 的充分必要条件为

$$(a_1,\cdots,a_n,m)|b.$$

若此条件成立, 则其解数(对模 m 不同余者)为 $m^{n-1}(a_1,\cdots,a_n,m)$.

证明　由定理 2.13 知, 对 $n=1$ 为真, 用数学归纳法证之, 命

$$(a_1,\cdots,a_n,m)=d\quad 及\quad (a_1,\cdots,a_{n-1},m)=d_1,$$

则

$$(d_1,a_n)=d.$$

由定理 2.13 知

$$a_nx_n+b\equiv 0\,(\mathrm{mod}\ d_1),\quad 0\leqslant x_n<m$$

有 $d\cdot\frac{m}{d_1}$ 个解, 对其中每个解 x_n, 命

$$a_nx_n+b=b_1d_1,$$

由归纳假定

$$a_1x_1+\cdots+a_{n-1}x_{n-1}+b_1d_1\equiv 0\,(\mathrm{mod}\ m)$$

之解数为

$$m^{n-2}(a_1,\cdots,a_{n-1},m)=m^{n-2}d_1,$$

故总解数为

$$\frac{md}{d_1} \cdot m^{n-2} \cdot d_1 = m^{n-1}d,$$

证毕.

设

$$f(x) = a_n x^n + \cdots + a_0$$

为一整系数多项式, 讨论同余方程

$$f(x) \equiv 0 \pmod{m}$$

的解. 若 x 为它的解, 则与 x 模 m 同余的整数都是它的解, 通常是考虑有多少个模 m 的剩余类适合上述方程.

高次同余方程的解数非常不规则, 例如,

(1) 同余方程 $x^3 - x = (x-1)(x+1)x \equiv 0 \pmod{6}$ 有六个解;

(2) 同余方程 $x^2 + 1 \equiv 0 \pmod{3}$ 无解;

(3) 同余方程 $(x-1)(x-p-1) \equiv 0 \pmod{p^2}$ 的解为 $1, p+1, 2p+1, \cdots, (p-1)p+1$, 共有 p 个解.

一般地, 若 $(m_1, m_2) = 1$, 则同余方程

$$f(x) \equiv 0 \pmod{m_1 m_2}$$

的解数为二方程

$$f(x) \equiv 0 \pmod{m_1}, \quad f(x) \equiv 0 \pmod{m_2}$$

解数之积, 利用孙子定理容易证明这个结论. 由此可见, 讨论方程

$$f(x) \equiv 0 \pmod{p^l}, \quad p\text{为素数}$$

的解数尤为重要.

定理 2.15 设 p 为素数, 同余方程

$$f(x) = a_n x^n + \cdots + a_0 \equiv 0 \pmod{p} \tag{2.8}$$

之解数 $\leqslant n$, 重解计算在内.

证明 可假定 $p \nmid a_n$, 若方程 (2.8) 无解, 则定理为真. 若 a 是一个解, 则可有

$$f(x) = (x-a) f_1(x) + r_1,$$

将 a 代入此式, 可见 $p|r_1$, 因而

$$f(x) \equiv (x-a) f_1(x) \pmod{p}.$$

若 a 又为 $f_1(x) \equiv 0 \pmod p$ 的解, 则同样可得

$$f_1(x) \equiv (x-a)f_2(x) \pmod p,$$

这时称 a 为 $f(x) \equiv 0 \pmod p$ 的重解. 若

$$f(x) \equiv (x-a)^k g_1(x) \pmod p,$$

$g_1(a) \not\equiv 0 \pmod p$, 则称 a 为 $f(x) \equiv 0 \pmod p$ 的 k 重解. 这时 $g_1(x)$ 的次数为 $n-k$.

设另有一个解 b, 则

$$0 \equiv f(b) \equiv (b-a)^k g_1(b) \pmod p,$$

因为 $p \nmid b-a$, 故

$$g_1(b) \equiv 0 \pmod p.$$

若 b 为 $g_1(x) \equiv 0 \pmod p$ 之 h 重解, 则同样有

$$f(x) \equiv (x-a)^k (x-b)^h g_2(x) \pmod p.$$

如此继续进行, 可得

$$f(x) \equiv (x-a)^k (x-b)^h \cdots (x-c)^l g(x) \pmod p,$$

$g(x)$ 的次数为 $n-k-h-\cdots-l$, 且

$$g(x) \equiv 0 \pmod p$$

不再有解, 定理即已证明.

定理 2.16　命

$$f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

若 $f(x) \equiv 0, f'(x) \equiv 0 \pmod p$ 无公共解, 则

$$f(x) \equiv 0 \pmod {p^l}$$

之解数等于

$$f(x) \equiv 0 \pmod p$$

之解数.

证明　利用数学归纳法, $l=1$ 时自不必证, 命 x_1 为

$$f(x)\equiv 0\,(\mathrm{mod}\ p^{l-1})$$

的解, 即 $f(x_1)=p^{l-1}s$, 则

$$f(x_1+p^{l-1}y)\equiv f(x_1)+p^{l-1}yf'(x_1)\,(\mathrm{mod}\ p^l)$$

(因对任意 n, $(x+p^{l-1}y)^n\equiv x^n+np^{l-1}y\,(\mathrm{mod}\ p^l)$), 但 $p\nmid f'(x_1)$, 所以有唯一之 $y_0\,(\mathrm{mod}\ p)$, 使 $s+y_0f'(x_1)\equiv 0\,(\mathrm{mod}\ p)$, 即

$$f(x_1+p^{l-1}y_0)\equiv 0\,(\mathrm{mod}\ p^l),$$

即证.

由定理 2.5, 同余方程

$$x^{p-1}\equiv 1\,(\mathrm{mod}\ p)$$

以 $1,2,3,\cdots,p-1$ 为解, 故

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-p+1)\,(\mathrm{mod}\ p).$$

以 $x=0$ 代入, 即得 $(-1)^{p-1}(p-1)!\equiv -1\,(\mathrm{mod}\ p)$.

定理 2.17 (Wilson 定理)　*若 p 为素数, 则*

$$(p-1)!\equiv -1\,(\mathrm{mod}\ p).$$

利用定理 2.16 可得如下定理.

定理 2.18　*若 p 为素数, 则同余方程*

$$x^{p-1}\equiv 1\,(\mathrm{mod}\ p^l)$$

有 $p-1$ 个解.

证明　取 $f(x)=x^{p-1}-1$, 则 $f'(x)=(p-1)x^{p-2}$, 方程 $f(x)\equiv 0\,(\mathrm{mod}\ p)$ 与方程 $f'(x)=-x^{p-2}\equiv 0\,(\mathrm{mod}\ p)$ 无公共解, 而前一方程有 $p-1$ 个解, 故定理得证.

2.5 原　根

在定理 2.18 中, 以 k 代替 $p-1$, 结果如何?

定理 2.19　*同余方程*

$$x^k\equiv 1\,(\mathrm{mod}\ p) \tag{2.9}$$

之解数为 $(k,p-1)$.

证明　设 $d=(k,p-1)$, 必有二整数 s 及 t 使

$$sk+t(p-1)=d.$$

如此, 则 $x^d=(x^k)^s\cdot(x^{p-1})^t$, 凡方程 (2.9) 的解一定是

$$x^d\equiv 1\,(\bmod\, p) \tag{2.10}$$

的解. 反之, 因 $d|k$, 则方程 (2,10) 的解也一定是方程 (2.9) 的解.

由定理 2.15, 已知方程 (2.10) 的解数不超过 d. 又 $x^{p-1}\equiv 1\,(\bmod\, p)$ 有 $p-1$ 个解, 再由定理 2.15, 同余方程

$$\frac{x^{p-1}-1}{x^d-1}=(x^d)^{\frac{p-1}{d}-1}+\cdots+x^d+1\equiv 0\,(\bmod\, p)$$

的解数不超过 $p-1-d$, 因而可见方程 (2.10) 恰有 d 个解.

定理 2.20　同余方程

$$x^k\equiv n\,(\bmod\, p),\quad p\nmid n$$

或无解, 或有 $(k,p-1)$ 个解.

证明　若有一解 x_0, 则

$$(x_0^{-1}x)^k\equiv x^k\cdot x_0^{-k}\equiv 1\,(\bmod\, p),$$

由定理 2.19 即得证.

定理 2.21　若 x 过模 p 之缩系, 则 x^k 取 $\dfrac{p-1}{(k,p-1)}$ 个模 p 不同的值.

证明　由定理 2.20, 有 $(k,p-1)$ 个不同余之数, 其 k 次方皆模 p 同余. 故全体 $p-1$ 个不同余之数分为 $\dfrac{p-1}{(k,p-1)}$ 类, 每一类对应一数, 模 p 皆不同余.

定义 2.1　设 h 为整数, $(h,n)=1$, 最小之正整数 l 使

$$h^l\equiv 1\,(\bmod\, n)$$

者, 称为 h 模 n 之次数 (或阶).

定理 2.22　若 $h^m\equiv 1\,(\bmod\, n)$, l 为 h 模 n 之次数, 则 $l|m$.

证明　必有两数 q 及 r 使 $m=ql+r$, $1\leqslant r<l$, 而

$$h^r\equiv h^m(h^l)^{-q}\equiv 1\,(\bmod\, n),$$

由 l 之定义, 必有 $r=0$, 证毕.

定理 2.23 设 $l|p-1$, 则模 p 的次数为 l 的互不同余的整数个数为 $\varphi(l)$.

证明 以 $\varphi_1(l)$ 表示模 p 的次数为 l 的互不同余的整数个数. 证明 $\varphi_1(l)$ 具有下述性质:

(1) 若 $(l_1,l_2)=1$, 则 $\varphi_1(l_1l_2)=\varphi_1(l_1)\varphi_1(l_2)$;

(2) 若 q 为素数, 则 $\varphi_1(q^r)=q^r-q^{r-1}$,

由此可知 $\varphi_l(l_1,l_2)=\varphi(l)$.

(1) 设 $(l_1,l_2)=1$, h_1 模 p 的次数为 l_1, h_2 模 p 的次数为 l_2, 令 $h=h_1h_2$, 设 h 模 p 的次数为 l, 易见

$$h^{l_1l_2}\equiv (h_1^{l_1})^{l_2}(h_2^{l_2})^{l_1}\equiv 1\,(\mathrm{mod}\ p),$$

故 $l|l_1l_2$. 由于

$$1\equiv (h_1h_2)^{ll_1}\equiv h_2^{ll_1}\,(\mathrm{mod}\ p),$$

所以 $l_2|ll_1$, 可见 $l_2|l$, 同样 $l_1|l$, 故 $l=l_1l_2$. 即由次数为 l_1 的数 h_1 与次数为 l_2 的数 h_2 产生一次数为 l_1l_2 的数 h_1h_2. 又若 h_1' 的次数也为 l_1, h_2' 的次数也为 l_2, 假设 $h_1h_2\equiv h_1'h_2'\,(\mathrm{mod}\ p)$, 则 $h_1^{-1}h_1'\equiv h_2{h_2'}^{-1}\,(\mathrm{mod}\ p)$, 但 ${h_1}^{-1}h_1'$ 的次数 $|l_1$, $h_2{h_2'}^{-1}$ 的次数 $|l_2$, 故必有

$$h_1^{-1}h_1'\equiv h_2{h_2'}^{-1}\equiv 1\,(\mathrm{mod}\ p),$$

即 $h_1\equiv h_1'$, $h_2\equiv h_2'$ $(\mathrm{mod}\ p)$. 所以由次数为 l_1 的数与次数为 l_2 的数按此法可生成 $\varphi_1(l_1)\cdot\varphi_1(l_2)$ 个次数为 l_1l_2 的数, 反之, 设 h 的次数为 l_1l_2, 必有二整数 s 和 t 使 $sl_1+tl_2=1$, 从而

$$h=h^{sl_1}\cdot h^{tl_2}.$$

今证 h^{sl_1} 的次数为 l_2(同样可证 h^{tl_2} 的次数为 l_1). 易见 $(h^{sl_1})^{l_2}\equiv 1\,(\mathrm{mod}\ p)$, 若 $(h^{sl_1})^r\equiv 1\,(\mathrm{mod}\ p)$, 则 $l_1l_2|sl_1r$, 亦即 $l_2|sr$, 由于 s 与 l_2 互素, 故 $l_2|r$, 可见 h^{sl_1} 的次数为 l_2, 到此, 证明了 $\varphi_1(l_1l_2)=\varphi_1(l_1)\cdot\varphi_1(l_2)$.

(2) 设 q 为素数, $l=q^r$, 则

$$x^{q^r}-1\equiv 0\,(\mathrm{mod}\ p)$$

的解数为 q^r, x 的次数必为 q^r 的因子, 若 x 适合此式, 但其次数不是 q^r, 则 x 必适合

$$x^{q^{r-1}}-1\equiv 0\,(\mathrm{mod}\ p),$$

此式有 q^{r-1} 个解, 故

$$\varphi_1(q^r)=q^r-q^{r-1},$$

定理证毕.

定义 2.2　次数为 $p-1$ 的数称为模 p 的一个原根 (或 p 的原根).

由定理 2.23 可知, p 有 $\varphi(p-1)$ 个原根, 若 g 为 p 的原根, 则

$$g^0,\quad g^1,\quad g^2,\cdots,\quad g^{p-2}\,(\bmod\ p)$$

为模 p 的一个缩系.

定义 2.3　任一整数 n $(p\nmid n)$, 必有一数 a, 使

$$n=g^a\,(\bmod\ p),\quad 0\leqslant a<p-1.$$

此 a 称为 n 模 p 的指数, 记为 $a=\mathrm{ind}_g n$.

注　在不引起混淆的情况下, 常记为 $\mathrm{ind}\,n$. 若 m 为任一数使 $n\equiv g^m\,(\bmod\ p)$, 则 $m\equiv \mathrm{ind}\ n\,(\bmod\ p-1)$.

指数与通常之对数有类似的性质:

(1) $\mathrm{ind}\ ab \equiv \mathrm{ind}\ a+\mathrm{ind}\ b\,(\bmod\ p-1),\ p\nmid ab$;

(2) $\mathrm{ind}\ a^l\equiv l\cdot\mathrm{ind}\ a\,(\bmod\ p-1), p\nmid a$.

定义 2.4　命 $p\nmid n$, 若

$$x^k\equiv n\,(\bmod\ p) \tag{2.11}$$

有解, 则 n 称为模 p 的 k 次剩余, 不然称为模 p 的 k 次非剩余.

定理 2.24　n 为模 p 的 k 次剩余的必要且充分条件为 $(k,p-1)$ 能整除 $\mathrm{ind}\ n$.

证明　式 (2.11) 等价于 $k\cdot\mathrm{ind}\ x\equiv \mathrm{ind}\ n\,(\bmod\ p-1)$, 此式有解的充分必要条件为 $(k,p-1)|\mathrm{ind}\ n$.

2.6　缩系的构造

设 m 为一自然数, 能否有一数 g 存在, 使

$$g^0,\quad g^1,\quad g^2,\cdots,\quad g^{\varphi(m)-1}\,(\bmod\ m)$$

为模 m 之缩系, 即模 m 的缩系能否由一个元素生成, 如果存在这样的生成元, 称它为 (模)m 的原根.

定理 2.25　m 有原根存在的充分必要条件为：$m=2,\,4,\,p^l$ 及$2p^l$(p为奇素数).

证明　(1) 设 m 的标准因子分解式为

$$m=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s},\quad p_1<p_2<\cdots<p_s.$$

任一整数 a, 若 $(a,p_i)=1$, 则

$$a^{\varphi(p_i^{l_i})}\equiv 1\,(\mathrm{mod}\ p_i^{l_i}).$$

命 l 为 $\varphi(p_1^{l_1}),\cdots,\varphi(p_s^{l_s})$ 的最小公倍数, 则

$$a^l\equiv 1\,(\mathrm{mod}\ m).$$

当 $l<\varphi(m)=\varphi(p_1^{l_1})\cdots\varphi(p_s^{l_s})$ 时, m 就没有原根. 若 $p_i>2,\varphi(p_i^{l_i})$ 为偶数, 则 m 不能有两个不同的奇素因子. 若 m 有原根, m 必为 $2^l,p^l$ 或 2^cp^l, 若 $c\geqslant 2,\varphi(2^c)=2^{c-1}$ 亦为偶数, 这时 2^cp^l 亦不能有原根. 故仅有 $m=2^l,p^l,2p^l$ 可能有原根.

(2) $m=2^l$, 若 $l=1$, 1 就是 2 的原根; 若 $l=2$, 3 是 4 的原根; 若 $l=3$,

$$1^2\equiv 3^2\equiv 5^2\equiv 7^2\equiv 1\,(\mathrm{mod}\ 8),$$

8 无原根. 当 $l\geqslant 3$ 时, 对任一奇数 a, 可以归纳证明 $a^{2^{l-2}}\equiv 1\,(\mathrm{mod}\ 2^l)$. 假设

$$a^{2^{l-3}}=1+2^{l-1}\lambda,\quad 2\nmid\lambda,$$

则

$$a^{2^{l-2}}=(1+2^{l-1}\lambda)^2\equiv 1\,(\mathrm{mod}\ 2^l),$$

故 2^l $(l\geqslant 3)$ 无原根.

(3) 若当 $m=p^l$, $l=1$ 时, 定理成立. 命 g 为 p 的原根, 若 $g^{p-1}\not\equiv 1\,(\mathrm{mod}\ p^2)$, 取 $r=g$, 若 $g^{p-1}\equiv 1\,(\mathrm{mod}\ p^2)$, 取 $r=g+p$, 今证 r 是 p^l 的原根. 设 d 为 r 模 p^l 的次数, 由于 $r^d\equiv 1\,(\mathrm{mod}\ p)$, r 是模 p 的原根, 故 $p-1|d$. 另一方面, 当 $r=g$ 时, 显然有 $r^{p-1}\not\equiv 1\,(\mathrm{mod}\ p^2)$, 而当 $r=g+p$ 时,

$$r^{p-1}-1=(g+p)^{p-1}-1=g^{p-1}+(p-1)pg^{p-2}-1\equiv -pg^{p-2}\not\equiv 0\,(\mathrm{mod}\ p^2),$$

命

$$r^{p-1}=1+kp,\quad p\nmid k,$$

因

$$(1+kp)^{p^s}\equiv 1+kp^{s+1}\,(\mathrm{mod}\ p^{s+2}),\quad s\geqslant 0,$$

故

$$(r^{p-1})^{p^s}\equiv 1+kp^{s+1}\,(\mathrm{mod}\ p^{s+2}),$$

即

$$r^{p^{l-2}(p-1)}\equiv 1+kp^{l-1}\not\equiv 1\,(\mathrm{mod}\ p^l),$$

可见 $d\nmid p^{l-2}(p-1)$. 由于 $d|p^{l-1}(p-1)$, $p-1|d$, 故 $d=\varphi(p^l)$, 即证得 p^l 有原根.

(4) 若 $m=2p^l$, 取 g 为 p^l 的原根, 若 g 为奇数, g 亦为 $2p^l$ 的原根, 若 g 为偶数, $g+p^l$ 就是 $2p^l$ 的原根. 证毕.

定理 2.26 若 $l>2$, 则 5 模 2^l 的次数为 2^{l-2}.

证明 当 $l\geqslant 3$ 时, 有

$$5^{2^{l-3}}\equiv 1+2^{l-1}\,(\mathrm{mod}\ 2^l).$$

当 $l=3$ 时上式成立, 再用归纳法

$$5^{2^{l-2}}=\left(5^{2^{l-3}}\right)^2\equiv\left(1+2^{l-1}+k\cdot 2^l\right)^2\equiv 1+2^l\,(\mathrm{mod}\ 2^{l+1}).$$

故 $5^{2^{l-3}}\not\equiv 1\,(\mathrm{mod}\ 2^l)$, 而 $5^{2^{l-2}}\equiv 1\,(\mathrm{mod}\ 2^l)$, 即 5 模 2^l 的次数为 2^{l-2}.

定理 2.27 设 $l>2$, 对任一奇数 a, 必有一 b 使

$$a\equiv(-1)^{\frac{a-1}{2}}\cdot 5^b\,(\mathrm{mod}\ 2^l),\quad b\geqslant 0.$$

证明 若 $a\equiv 1\,(\mathrm{mod}\ 4)$, 由定理 2.26 知

$$5^b,\quad 0\leqslant b<2^{l-2}$$

为 2^{l-2} 个模 2^l 不同余的数, 且皆 $\equiv 1\,(\mathrm{mod}\ 4)$, 故必有一 b 使 $a\equiv 5^b\,(\mathrm{mod}\ 2^l)$.

若 $a\equiv 3\,(\mathrm{mod}\ 4)$, 则 $-a\equiv 1\,(\mathrm{mod}\ 4)$, 由上述即得所求.

定理 2.28 设 $m=2^l\cdot p_1^{l_1}\cdots p_s^{l_s}$(标准分解式), $l\geqslant 0, l_1>0,\cdots,l_s>0$, 依 $l=0,1$; $l=2$ 或 $l>2$ 以定义 $\delta=0,1$ 或 2, 则 m 之缩系可由 $s+\delta$ 个数之乘方之积表出.

证明 (1) 设 $m=m'm'', (m',m'')=1$, 命

$$a_1,\cdots,a_{\varphi(m')}$$

为 m' 的缩系, 且 $a_i\equiv 1\,(\mathrm{mod}\ m'')$(这总是可能的), 又命

$$b_1,\cdots,b_{\varphi(m'')}$$

为 m'' 的缩系, 且 $b_i\equiv 1\,(\mathrm{mod}\ m')$, 则

$$a_ib_j,\quad 1\leqslant i\leqslant\varphi(m'),\quad 1\leqslant j\leqslant\varphi(m''),$$

即表 $m'm''$ 之缩系.

(2) 由定理 2.25 和定理 2.27 可知, p^l $(l>2)$ 的缩系由一个数之乘方组成, 2^l 的缩系由 δ 个数的乘方之积组成, 可见定理成立.

习　题

习题 2.1　试证: $3x^2+2=y^2$ 无整数解.

习题 2.2　设 p 为素数, $1\leqslant k<p-1$, 试证: $p\left|\binom{p}{k}\right.$ (二项式系数), 由此推出

$$(a+b)^p\equiv a^p+b^p\,(\mathrm{mod}\ p).$$

习题 2.3　证明: $\sum\limits_{d|m}\varphi(d)=m$.

习题 2.4　命 s 为 (m,n) 中不同素因子之积, 则

$$\frac{\varphi(mn)}{\varphi(m)\varphi(n)}=\frac{s}{\varphi(s)}.$$

习题 2.5　设 g 与 g_1 均为素数 p 的原根, 且 $g_1=g^b\,(\mathrm{mod}\ p)$, 则

$$\mathrm{ind}_g n\equiv\mathrm{ind}_{g_1}n\cdot\mathrm{ind}_g g_1\,(\mathrm{mod}\ p-1).$$

习题 2.6　证明:

(1) $\varphi(n)=\dfrac{1}{2}n$ 当且仅当 $n=2^k$, $k\in\mathbb{N}$;

(2) $\varphi(n)=\dfrac{1}{3}n$ 当且仅当 $n=2^k\cdot 3^i$, $k,i\in\mathbb{N}$.

习题 2.7　设 $p=2^{2^n}+1$ 为 Fermat 素数, 试证 3 为 p 的原根.

习题 2.8　设 p 为一奇素数, 试证当且仅当对 $p-1$ 所有的素因子 q 有 $a^{\frac{(p-1)}{q}}\not\equiv 1\ (\mathrm{mod}\ p)$ 时, a 为 p 的原根.

习题 2.9　定义莫比乌斯函数 μ 为

$$\mu(n)=\begin{cases}1, & n=1,\\ 0, & n\text{有平方因子},\\ (-1)^s, & n=p_1\cdots p_s.\end{cases}$$

证明:

(1) 若 $n>1$, 有 $\sum\limits_{d|n}\mu(d)=0$;

(2) $n=\sum\limits_{d|n}\mu(d)\cdot\varphi\left(\dfrac{n}{d}\right)$.

习题 2.10　将同余的概念类比在 $\mathbb{Z}[\mathrm{i}]$ 中定义, 证明任意 $\mathbb{Z}[\mathrm{i}]$ 中一个元素 $a+b\mathrm{i}\equiv 0$ 或 $1(\mathrm{mod}\ 1+\mathrm{i})$.

习题 2.11 将同余的概念类比在 $\mathbb{Z}[\omega]$ 中定义, 证明 $\mathbb{Z}[\omega]$ 中任一元素 $a+b\omega \equiv 0, 1, -1 \pmod{1-\omega}$.

习题 2.12 令 $\lambda = 1-\omega \in \mathbb{Z}[\omega]$, 若 $\alpha \in \mathbb{Z}[\omega]$ 满足 $\alpha \equiv 1 \pmod{\lambda}$, 证明

$$\alpha^3 \equiv 1 \pmod{9}.$$

习题 2.13 设 p 是素数, 证明: 若 q 是 $2^p - 1$ 的一个因子, 那么

(1) $q \equiv 1 \pmod{p}$;

(2) $q \equiv \pm 1 \pmod{8}$.

习题 2.14 证明若 q 是 $F_K = 2^{2^k} + 1$ 的一个正因子, 那么 $q \equiv 1 \pmod{2^{k+1}}$. 进一步, 若 $k \geqslant 2$, 那么 $q \equiv 1 \pmod{2^{k+2}}$.

习题 2.15 证明若 $l \geqslant 1$ 且 $a \equiv b \pmod{p^l}$, 那么 $a^p \equiv b^p \pmod{p^{l+1}}$.

习题 2.16 令 p 是奇素数且 $l \geqslant 2$, 试证对任意 $a \in \mathbb{Z}$, 有

$$(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-2} \pmod{p^l}.$$

习题 2.17 由孙子定理求同余方程组的解

$$\begin{cases} x \equiv 1 \pmod{7}, \\ x \equiv 4 \pmod{9}, \\ x \equiv 3 \pmod{5}. \end{cases}$$

习题 2.18 解同余方程组的解

$$\begin{cases} x \equiv 1 \pmod{6}, \\ x \equiv 4 \pmod{9}, \\ x \equiv 7 \pmod{15}. \end{cases}$$

第3章　二次剩余

3.1　定义及 Euler 判别条件

设 m 为大于 1 的正整数, n 与 m 互素, 若

$$x^2 \equiv n \pmod m$$

可解, 则 n 称为模 m 的二次剩余, 否则称为非二次剩余.

例如, $1,2,4$ 为模 7 的二次剩余, $3,5,6$ 为模 7 的二次非剩余.

设 p 为奇素数, $p \nmid n$, 定义 Legendre 符号:

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & n \text{ 为模 } p \text{ 的二次剩余}, \\ -1, & n \text{ 为模 } p \text{ 的非二次剩余}. \end{cases}$$

当 $n \equiv n' \pmod p$ 时, 显然有

$$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right).$$

定理 3.1　设 p 为奇素数, 模 p 的缩系中有 $\frac{1}{2}(p-1)$ 个二次剩余, 有 $\frac{1}{2}(p-1)$ 个二次非剩余, 且

$$1^2, \quad 2^2, \cdots, \quad \left(\frac{1}{2}(p-1)\right)^2,$$

即为所有的模 p 二次剩余.

证明　若二次方程

$$x^2 \equiv n \pmod p \tag{3.1}$$

有解, 则至多有两个解. 由

$$(p-x)^2 \equiv (-x)^2 \equiv n \pmod p$$

可知, 式 (3.1) 必有一根适合

$$1 \leqslant x \leqslant \frac{1}{2}(p-1). \tag{3.2}$$

又因为

$$a^2 - b^2 = (a+b)(a-b),$$

当 $a^2 \equiv b^2 \pmod p$ 时, $a+b$ 与 $a-b$ 中必有一数是 p 的倍数, 由此可知

$$1^2, \quad 2^2, \cdots, \quad \left(\frac{1}{2}(p-1)\right)^2,$$

模 p 两两不同余, 故得定理.

定理 3.2(Euler 判别条件)　设 p 为奇素数, $p \nmid n$, 则

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod p.$$

证明　(1) 若 $\left(\frac{n}{p}\right) = 1$, 则有整数 x 使 $x^2 \equiv n \pmod p$, 由 Euler 定理知

$$n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p.$$

(2) 由定理 2.15 知, 方程 $x^{\frac{p-1}{2}} \equiv 1 \pmod p$ 的解数 $\leqslant \frac{1}{2}(p-1)$, 由上面定理可知, 它有 $\frac{1}{2}(p-1)$ 个解, 它们是模 p 的所有的二次剩余, 而且没有其他解.

(3) 由于 $n^{p-1} \equiv 1 \pmod p$, 所以

$$p|(n^{p-1}-1) = (n^{\frac{1}{2}(p-1)}-1)(n^{\frac{1}{2}(p-1)}+1).$$

若 $p \nmid n^{\frac{1}{2}(p-1)}-1$, 则 $p|n^{\frac{1}{2}(p-1)}+1$, 即 $n^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod p$, 当 n 为模 p 的二次非剩余时, 就有 $n^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$, 证毕.

定理 3.3　若 $p \nmid mn, p > 2$, 则

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right),$$

即Legendre符号是积性函数.

证明　因为

$$\left(\frac{mn}{p}\right) = (mn)^{\frac{p-1}{2}} = m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod p,$$

两端都为 ± 1, $p > 2$, 故定理成立.

由定理 3.3 可知, 两二次剩余之积为二次剩余, 两非二次剩余之积为二次剩余, 一二次剩余与一非二次剩余之积为非二次非剩余.

3.2　Legendre 符号

由定理 3.3 可知, 如能计算

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{q}{p}\right) \quad (q\text{为奇素数}),$$

就能计算一切的二次剩余. 若 $n=\pm 2^m q_1^{l_1}\cdots q_s^{l_s}$, 则

$$\left(\frac{n}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m\left(\frac{q_1}{p}\right)^{l_1}\cdots\left(\frac{q_s}{p}\right)^{l_s}.$$

由定理 3.2 知

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\,(\mathrm{mod}\ p),$$

由于等式两端均为 ± 1, 故得如下定理.

定理 3.4 若 p 为奇素数, 则

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

当 $p\equiv 1\,(\mathrm{mod}\ 4)$ 时, -1 为模 p 的二次剩余, 当 $p\equiv 3\,(\mathrm{mod}\ 4)$ 时, -1 为模 p 的二次非剩余.

定理 3.5(Gauss 引理) 命 p 为奇素数, $p\nmid n$, 设 $\frac{1}{2}(p-1)$ 个数

$$n,\quad 2n,\cdots,\quad \frac{1}{2}(p-1)n$$

的最小正余数中有 m 个大于 $\frac{p}{2}$, 则

$$\left(\frac{n}{p}\right)=(-1)^m.$$

例如，$p=7, n=10$, 因 $10,20,30\equiv 3,6,2\,(\mathrm{mod}\ 7)$ 只有 $6>\frac{p}{2}$, 故

$$m=1,\quad \left(\frac{10}{7}\right)=-1.$$

证明 以 $a_1,a_2,\cdots,a_l\left(l=\frac{1}{2}(p-1)-m\right)$ 表示诸余数中小于 $\frac{p}{2}$ 者, 以 b_1, $b_2,\cdots,b_m$ 表示诸余数中大于$\frac{p}{2}$ 者, 则 $a_1,a_2,\cdots,a_l,p-b_1,p-b_2,\cdots,p-b_m$ 都在 1 与 $\frac{1}{2}(p-1)$ 之间, 它们是两两不同的, 若

$$a_s=p-b_t,$$

则 $a_s+b_t=p$, 因而存在 x 和 y, 使

$$xn+yn\equiv 0\,(\mathrm{mod}\ p),\quad 1\leqslant x,y\leqslant\frac{1}{2}(p-1),$$

由于 $p\nmid n$, 故 $p|x+y$, 这是不可能的, 所以

$$\prod_{s=1}^{l} a_s \prod_{t=1}^{m} (p - b_t) = \left(\frac{p-1}{2}\right)!.$$

上式左端

$$(-1)^m \prod_{s=1}^{l} a_s \cdot \prod_{t=1}^{m} b_t = (-1)^m \prod_{k=1}^{\frac{1}{2}(p-1)} kn = (-1)^m \left(\frac{p-1}{2}\right)! n^{\frac{p-1}{2}} \pmod p,$$

故得

$$n^{\frac{p-1}{2}} \equiv (-1)^m \pmod p,$$

由 Euler 判别条件知

$$\left(\frac{n}{p}\right) = (-1)^m.$$

在定理 3.5 中, 取 $n = 2$,

$$2, \quad 2 \cdot 2, \quad 2 \cdot 3, \cdots, \quad 2 \cdot \frac{p-1}{2}$$

都在 1 与 p 之间, 设 $\frac{p}{2} < 2k < p$, 则 $\frac{p}{4} < k < \frac{p}{2}$, 所以 $m = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right]$, 设 $p = 8a + r$, $r = 1, 3, 5, 7$, 则得

$$m = 2a + \left[\frac{r}{2}\right] - \left[\frac{r}{4}\right] \equiv 0, 1, 1, 0 \pmod 2,$$

故得如下定理.

定理 3.6 若 p 为奇素数, 则

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)},$$

即当 $p \equiv \pm 1 \pmod 8$ 时, 有 $(-1)^m = 1$, $\left(\frac{2}{p}\right) = 1$, 于是 2 为模 p 二次剩余; 当 $p \equiv \pm 3 \pmod 8$ 时, 有 $(-1)^m = -1$, $\left(\frac{2}{p}\right) = -1$, 于是 2 为模 p 非二次剩余.

定理 3.7(二次互反律) 设 p, q 为奇素数, $p \neq q$, 则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

证明 设 $1 \leqslant k \leqslant \frac{1}{2}(p-1)$, 用带余除法得

$$kq = q_k p + r_k, \quad q_k = \left[\frac{kq}{p}\right], \quad 0 \leqslant r_k < p.$$

令

$$a = \sum_{s=1}^{l} a_s, \quad b = \sum_{t=1}^{m} b_t$$

(a_s 与 b_t 的定义见定理 3.5), 则

$$\sum_{k=1}^{\frac{1}{2}(p-1)} r_k = a + b.$$

在定理 3.5 中已证明, $a_s, p - b_t$ 与 $1, 2, \cdots, \frac{1}{2}(p-1)$ 相同, 即

$$\frac{p^2-1}{8} = 1 + 2 + \cdots + \frac{1}{2}(p-1) = \sum_{s=1}^{l} a_s + \sum_{t=1}^{m} (p - b_t) = a + mp - b,$$

又

$$\frac{p^2-1}{8} q = p \sum_{k=1}^{\frac{1}{2}(p-1)} q_k + \sum_{k=1}^{\frac{1}{2}(p-1)} r_k = p \sum_{k=1}^{\frac{1}{2}(p-1)} q_k + a + b,$$

两式相减得

$$\frac{p^2-1}{8}(q-1) = p \sum_{k=1}^{\frac{1}{2}(p-1)} q_k - mp + 2b.$$

因 $q > 2$, 故

$$m \equiv \sum_{k=1}^{\frac{1}{2}(p-1)} q_k = \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{qk}{p}\right] \pmod 2,$$

则有

$$\left(\frac{q}{p}\right) = (-1)^m = (-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{qk}{p}\right]}.$$

同法可得

$$\left(\frac{p}{q}\right) = (-1)^{\sum\limits_{l=1}^{\frac{1}{2}(q-1)} \left[\frac{lp}{q}\right]}.$$

于是

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{kq}{p}\right] + \sum\limits_{l=1}^{\frac{1}{2}(q-1)} \left[\frac{lp}{q}\right]}.$$

利用以下的引理 3.1, 定理 3.7 就能得证.

引理 3.1

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

证明　以 $(0,0)$, $\left(0,\dfrac{1}{2}q\right)$, $\left(\dfrac{1}{2}p,0\right)$, $\left(\dfrac{1}{2}p,\dfrac{1}{2}q\right)$ 为顶点作长方形, 如图 3-1 所示.

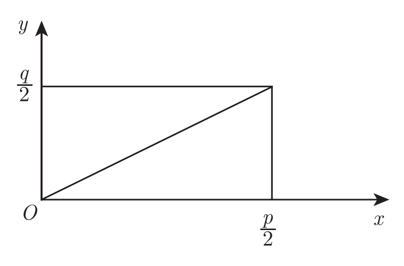


图 3-1

长方形内的整点 (两坐标都为整数) 个数为 $\dfrac{p-1}{2}\cdot\dfrac{q-1}{2}$, 在下三角形内整点的个数为

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right],$$

在上三角形内的整点个数为

$$\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right],$$

引理证毕.

例 3.1　求以 3 为二次剩余的素数 $p\ (>3)$.

解　由互反律

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)},$$

因

$$\left(\frac{p}{3}\right)=\begin{cases}1, & p\equiv 1\ (\mathrm{mod}\ 3),\\ -1, & p\equiv 2\ (\mathrm{mod}\ 3),\end{cases}$$

$$(-1)^{\frac{1}{2}(p-1)}=\begin{cases}1, & p\equiv 1\ (\mathrm{mod}\ 4),\\ -1, & p\equiv 3\ (\mathrm{mod}\ 4),\end{cases}$$

由孙子定理立即可以算出

$$\left(\frac{3}{p}\right)=\begin{cases}1, & p\equiv \pm 1\ (\mathrm{mod}\ 12),\\ -1, & p\equiv \pm 5\ (\mathrm{mod}\ 12).\end{cases}$$

例 3.2 同余方程

$$x^2 \equiv -1457 \pmod{2389}$$

是否可解?

解 令 $p = 2389$, 它是一个素数, $1457 = 31 \times 47$,

$$\begin{aligned}
&\left(\frac{-1}{p}\right) = 1,\\
&\left(\frac{31}{p}\right) = \left(\frac{p}{31}\right) = \left(\frac{31 \times 77 + 2}{31}\right) = \left(\frac{2}{31}\right) = 1,\\
&\left(\frac{47}{p}\right) = \left(\frac{p}{47}\right) = \left(\frac{39}{47}\right) = \left(\frac{3}{47}\right)\left(\frac{13}{47}\right) = -\left(\frac{47}{3}\right)\left(\frac{47}{13}\right)\\
&\qquad = -\left(\frac{2}{3}\right)\left(\frac{8}{13}\right) = -\left(\frac{2}{3}\right)\left(\frac{2}{13}\right) = -1,
\end{aligned}$$

所以 $\left(\frac{-1457}{2389}\right) = -1$, 同余式无解.

3.3 Jacobi 符 号

设 m 为正奇数, $m = \prod_{r=1}^{t} p_r$, p_r 为素数, 可以重复出现, 若 $(n, m) = 1$, 定义

$$\left(\frac{n}{m}\right) = \prod_{r=1}^{t} \left(\frac{n}{p_r}\right),$$

称为 Jacobi 符号.

显然有 $\left(\frac{1}{m}\right) = 1$, $\left(\frac{a^2}{m}\right) = 1$, 如果 $n \equiv n' \pmod{m}$, 以及 $(n, m) = 1$, 则

$$\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right).$$

若 $(n, m) = (n, m') = 1$, m' 也是正奇数, 则有

$$\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right).$$

若 $(n, m) = (n', m) = 1$, 则

$$\left(\frac{nn'}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right).$$

定理 3.8 $\left(\frac{-1}{m}\right) = (-1)^{\frac{1}{2}(m-1)}$.

证明　只需证明

$$\sum_{i=1}^{t}\frac{p_i-1}{2}\equiv\frac{\left(\prod_{i=1}^{t}p_i-1\right)}{2}\,(\bmod\ 2)$$

即可. 因为

$$(p_1-1)(p_2-1)\equiv 0\,(\bmod\ 4),$$

故

$$p_1p_2-1\equiv p_1-1+p_2-1\,(\bmod\ 4),\quad \frac{p_1p_2-1}{2}\equiv\frac{p_1-1}{2}+\frac{p_2-1}{2}\,(\bmod\ 2),$$

由归纳法即可证.

定理 3.9　$\left(\dfrac{2}{m}\right)=(-1)^{\frac{1}{8}(m^2-1)}$.

证明　$\left(\dfrac{2}{m}\right)=\prod\limits_{i=1}^{t}\left(\dfrac{2}{p_i}\right)=\prod\limits_{i=1}^{t}(-1)^{\frac{1}{8}(p_i^2-1)}=(-1)^{\sum\limits_{i=1}^{t}\frac{p_i^2-1}{8}}$,

因 $8|p_i^2-1$, 故

$$(p_1^2-1)(p_2^2-1)\equiv 0\,(\bmod\ 16),$$

$$p_1^2p_2^2-1\equiv p_1^2-1+p_2^2-1\,(\bmod\ 16),$$

$$\frac{p_1^2p_2^2-1}{8}\equiv\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}\,(\bmod\ 2).$$

由归纳法可证

$$\sum_{i=1}^{t}\frac{p_i^2-1}{8}\equiv\frac{\prod\limits_{i=1}^{t}p_i^2-1}{8}\equiv\frac{m^2-1}{8}\,(\bmod\ 2),$$

定理得证.

定理 3.10　若 m 与 n 为二正奇数, 且 $(m,n)=1$, 则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

证明　令 $m=\prod p, n=\prod q$, 则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\left(\prod_p\prod_q\left(\frac{p}{q}\right)\right)\cdot\left(\prod_p\prod_q\left(\frac{q}{p}\right)\right)$$

$$= \prod_p \prod_q \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \prod_p \prod_q (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$
$$= (-1)^{\sum\limits_p \frac{p-1}{2}\cdot\sum\limits_q \frac{q-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

例如, $\left(\frac{383}{443}\right) = \left(\frac{443}{383}\right)(-1)^{221\times 191}$

$$= -\left(\frac{60}{383}\right) = -\left(\frac{2^2}{383}\right)\left(\frac{15}{383}\right)$$
$$= \left(\frac{383}{15}\right) = \left(\frac{8}{15}\right) = \left(\frac{2}{15}\right) = 1.$$

3.4　二次剩余假设

设 $n = pq$, p 和 q 为奇素数. 定义 $\mathbb{Z}_n^* = \{x \mid (x,n)=1,\ 1 \leqslant x < n\}$. 由 Jacobi 符号的定义, 若 $a \in \mathbb{Z}_n^*$, 则

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right).$$

当同余方程 $x^2 \equiv a \pmod n$ 可解时, 称 a 为模 n 的二次剩余, 否则称 a 为模 n 的非二次剩余. 当 a 为模 n 的二次剩余时, a 同时也是模 p 和模 q 的二次剩余, 从而

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1.$$

反之, 若 $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, 可见 $x^2 \equiv a \pmod p$ 和 $x^2 \equiv a \pmod q$ 都可解, 由中国剩余定理可知 $x^2 \equiv a \pmod n$ 可解, a 为模 n 的二次剩余.

若

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1,$$

这时 a 同时是模 p 和模 q 的非二次剩余, 因而 a 是模 n 的非二次剩余. 但这时有 $\left(\frac{a}{n}\right) = 1$. 定义集合

$$\mathbb{Z}_n^1 = \left\{ a \in \mathbb{Z}^* \;\middle|\; \left(\frac{a}{n}\right) = 1 \right\},$$

利用中国剩余定理, 可知 $\mathbb{Z}_n^1$ 中模 n 的二次剩余个数和非二次剩余个数都为

$$(p-1)(q-1)/4.$$

当 $p \equiv q \equiv 3 \pmod 4$ 时, n 称为 Blum 数, 这时

$$\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = -1, \quad \left(\frac{-1}{n}\right) = 1.$$

可见, -1 是 $\mathbb{Z}_n^1$ 中的一个非二次剩余. 任取 $s \in \mathbb{Z}_n^*$, $s^2 \in \mathbb{Z}_n^1$ 一定是二次剩余, 而 $-s^2$ 一定是非二次剩余.

引理 3.2　任一模 n 的二次剩余有四个模 n 的平方根.

证明　设 a 为模 n 的二次剩余, $x^2 \equiv a \pmod p$ 的两个解为 $\pm x_0$, $x^2 \equiv a \pmod q$ 的两个解为 $\pm x_1$, 则下述四个方程组

$$\begin{cases} y_1 \equiv x_0 \pmod p, \\ y_1 \equiv x_1 \pmod q, \end{cases} \quad \begin{cases} y_1 \equiv -x_0 \pmod p, \\ y_1 \equiv -x_1 \pmod q, \end{cases}$$

$$\begin{cases} y_1 \equiv x_0 \pmod p, \\ y_1 \equiv -x_1 \pmod q, \end{cases} \quad \begin{cases} y_1 \equiv -x_0 \pmod p, \\ y_1 \equiv x_1 \pmod q \end{cases}$$

各有一个解

$$y_1 \pmod n, \quad y_2 \equiv -y_1 \pmod n, \quad y_3 \pmod n, \quad y_4 \equiv -y_3 \pmod n,$$

它们是 $x^2 \equiv a \pmod n$ 的四个解. 证毕.

定理 3.11　给定 $x, y \in \mathbb{Z}_n^*$, 若 $x^2 \equiv y^2 \pmod n$, $x \not\equiv \pm y \pmod n$, 则存在一个 n 因子分解的多项式时间算法.

证明　由于 $0 \equiv x^2 - y^2 \equiv (x+y)(x-y) \pmod n$, 且 $x \not\equiv \pm y \pmod n$, 可知 n 与 $x \pm y$ 的最大公因子一定是 n 的素因子, 而计算最大公因子是一个多项式时间算法. 证毕.

定理 3.11 表明, 求解 $x^2 \equiv a \pmod n$ 的计算复杂度不低于 n 因子分解的计算复杂度, 因而前者也是一个困难的问题.

定理 3.12　若已知 $n = pq$ 的因子分解, 则存在一个计算复杂度为 $O(\lg^3(n))$ 的多项式时间算法判断任一 $a \in \mathbb{Z}_n^1$ 是否为模 n 的二次剩余.

证明　若 $a \in \mathbb{Z}_n^1$. 当 $\left(\dfrac{a}{p}\right) = 1$ 时, a 为模 n 的二次剩余; 当 $\left(\dfrac{a}{p}\right) = -1$ 时, a 为模 n 的非二次剩余. 由定理 3.10 知, 计算 $\left(\dfrac{a}{p}\right)$ 相当于计算一次辗转相除法, 其计算量为 $O(\lg^3(n))$, 证毕.

二次剩余假设: 若不知道 $n = pq$ 的因子分解, 判断 $a \in \mathbb{Z}_n^1$ 是否为模 n 的二次剩余是一个困难问题.

定理 3.12 表明, 当 n 的因子分解已知时, 存在多项式时间复杂度为 $O(\lg^3(n))$ 的算法判断 $a \in \mathbb{Z}_n^1$ 是否是二次剩余. 称上述问题是带陷门的. 在 8.5 节, 将基于判断二次剩余的困难性构造一个公钥密码.

为了使用方便, 将二次剩余假设作更确切的表述.

设 k 是正整数, 定义

$$H_k = \left\{ n \middle| n = pq,\ |p| = |q| = k,\ p,\ q\text{为素数} \right\}$$

表示因子分解困难的整数集合, 其中 $|p|$ 为 p 的二进制表示的长度. 对任一 $x \in \mathbb{Z}_n^1$, 定义映射

$$Q_n(x) = \begin{cases} 1, & x\text{ 为模 } n \text{ 的二次剩余}, \\ 0, & x\text{ 为模 } n \text{ 的非二次剩余}. \end{cases}$$

本节以下所提及的多项式的系数都是非负实数, 次数都为正的.

定义 3.1(二次剩余假设) 设 P 为一给定多项式, 函数 $C(n, x):\ \mathbb{N}\times\mathbb{N} \to \{0, 1\}$, n, x 表示为 $2k$ 长的比特串, C 为有 $4k$ 比特输入的布尔函数. 假设函数 $C(n, x)$ $(n \in H_k,\ x \in \mathbb{Z}_n^1)$ 对于 H_k 中至少 $1/P(k)$ 部分的 n, 有 $C(n, x) = Q_n(x)$. 令 c_k 表示函数 C 的最小门数 (任一布尔函数可以用有限个与门、或门和非门组成的门电路来实现), 则对任一多项式 $L(k)$, 存在正整数 D, 当 $k > D$ 时有 $c_k > L(k)$.

上述假设中, 是对 n 平均来说的, 判断 $a \in \mathbb{Z}_n^1$ 是否是二次剩余是一个困难问题.

若存在一多项式 $L'(k)$, 当 k 足够大时有 $c_k < L'(k)$, 则称函数 $C(n, x)$ 的大小是多项式有界的.

定义 3.2 设 $\varepsilon > 0$, $C(x)$ 为 $\mathbb{Z}_n^1 \to \{0, 1\}$ 的函数, 若对 $\mathbb{Z}_n^1$ 中至少 $\left(\dfrac{1}{2} + \varepsilon\right)$ 部分的 x 有 $C(x) = Q_n(X)$, 则称 C 为 Q_n 的 ε-逼近.

令

$$B_k = \left\{ Q_n : \mathbb{Z}_n^1 \to \{0, 1\} \,\middle|\, n \in H_k \right\},$$

Q_n 称为一个区分函数. 定义区分函数簇

$$B = \bigcup_{k \in N'} B_k,$$

这是 N' 表示一自然数子集合.

定义 3.3(不可逼近区分函数簇) 设 P_1, P_2 为两个多项式, $k \in N'$. 假设对 H_k 中至少 $1/P_1(k)$ 部分的 n, 函数 $C(n, x)$ 是 $Q_n(x)$ 的 $(1/P_2(k))$-逼近, 以 c_k 表示函数 C 的最小门数. 若对任一多项式 $L(k)$, 当 k 足够大时有 $c_k > L(k)$, 则称 B 为不可逼近区分函数簇.

若存在一个多项式 P, 对任一输入 n, 算法 C 一定在不超过 $P(k)$ 步之内完成计算, 且输出结果一定正确, 则称 C 为确定型多项式时间算法. 若对任一输入 n, C 一定在不超过 $P(k)$ 步之内完成计算, 但输出结果有一定的差错误差, 则称 C 为概

率多项式时间算法. 这类算法是不确定型的, 在计算过程中每一状态可能有几个可选择的下一状态. 若一概率多项式时间算法任一输出的成功概率为 $1-\delta(k)$, 而对任一多项式 Q, 当 k 足够大时有 $\delta(k) \leqslant 1/Q(k)$, 则称该概率多项式时间算法以可以忽略的差错概率给出计算结果.

定理 3.13　设 P_1, P_2 为多项式, $k \in N'$, 假设 S 为因子分解困难的整数集合. 如果对任一 $n \in S$, 函数 $C(n,x)$ 是 $Q_n(x)$ 的 $(1/P_1(k))$-逼近, 则基于函数 $C(n,x)$ 可以构造一个概率多项式时间算法 $G(n,x)$, 它对任一 $n \in S$ 及任一 $x \in \mathbb{Z}_n^1$, 以大于 $1-1/P_2(k)$ 的概率正确判断 x 是否为模 n 的二次剩余.

引理 3.3(弱大数定理)　设 $y_1, y_2, \cdots, y_r$ 为 r 个相互独立的 0-1 随机变量, 记 $p = \Pr(y_i = 1)\ (1 \leqslant i \leqslant r)$. 令 $S = \sum\limits_{i=1}^{r} y_i$, 则对于两个实数 $\psi, \delta, r \geqslant 1/4\delta\psi^2$, 有

$$\Pr(|S/r - p| \geqslant \psi) \leqslant \delta$$

(注意: r 以 δ^{-1}, ψ^{-1} 的多项式为下界)

证明　设 X 为随机变量, 则有 Chebyshev 不等式

$$\Pr(|X - E(X)| \geqslant \psi) \leqslant \frac{\mathrm{Var}(X)}{\psi^2}.$$

这里 $E(X)$ 表示 X 的数学期望, $\mathrm{Var}(X) = E((X - E(X))^2)$ 表示 X 的均方差.

令 $X = S/r$, 易见

$$\begin{aligned} E(X) &= E(y_i) = p \quad (1 \leqslant i \leqslant r), \\ \mathrm{Var}(y_i) &= E((y_i - p)^2) = E(y_i^2 - 2py_i + p^2) \\ &= E(y_i^2) - p^2 = p(1-p) \leqslant \frac{1}{4}. \end{aligned}$$

记 $\overline{y}_i = y_i - p$, 易见 $E(\overline{y}_i) = 0$. 由定义

$$\begin{aligned} \mathrm{Var}(X) &= E\left(\left(\sum y_i/r - p\right)^2\right) = \frac{1}{r^2}E\left(\left(\sum (y_i - p)\right)^2\right) \\ &= \frac{1}{r^2}E\left(\left(\sum_{i=1}^{n} \overline{y}_i\right)^2\right) = \frac{1}{r^2}E\left(\sum_{i=1}^{n} \overline{y}_i^2 + \sum_{1 \leqslant i \neq j \leqslant r} \overline{y}_i\,\overline{y}_j\right) \\ &= \frac{1}{r^2}\sum_{i=1}^{r}((y_i - p)^2) + \sum_{1 \leqslant i \neq j \leqslant r} E(\overline{y}_i)E(\overline{y}_j) \\ &= \frac{1}{r}\mathrm{Var}(y_i) = \frac{p(1-p)}{r} \leqslant \frac{1}{4r}. \end{aligned}$$

因 $\overline{y}_i$ 与 $\overline{y}_j$ 为独立随机变量, 以上利用了 $E(\overline{y}_i\overline{y}_j) = E(\overline{y}_i)E(\overline{y}_j) = 0$. 最后, 由 Chebyshev 不等式及条件 $r \geqslant 1/4\delta\psi^2$ 得

$$\Pr(|S/r - p| \geqslant \psi) \leqslant \frac{1}{4r\psi^2} \leqslant \delta.$$

引理得证.

定理 3.13 的证明 令

$$\alpha = \Pr(C(n,x)=1 \mid Q_n(x)=1), \quad \beta = \Pr(C(n,x)=1 \mid Q_n(x)=0),$$

则

$$\begin{aligned}
&\Pr(C(n,x)=Q_n(x) \mid x \in \mathbb{Z}_n^1) \\
=& \Pr(Q_n(x)=1 \mid x \in \mathbb{Z}_n^1)\Pr(C(n,x)=1 \mid Q_n(x)=1) \\
&+ \Pr(Q_n(x)=0 \mid x \in \mathbb{Z}_n^1)\Pr(C(n,x)=0 \mid Q_n(x)=0) \\
=& \frac{\alpha}{2} + \frac{1-\beta}{2} = \frac{1}{2} + \frac{\alpha-\beta}{2}.
\end{aligned}$$

记

$$\varepsilon = \frac{1}{P_1(k)}, \quad \delta = \frac{1}{P_2(k)},$$

由于 $C(n,x)$ 是 $Q_n(x)$ 的 ε-逼近, 可见 $\alpha - \beta \geqslant 2\varepsilon$.

在 $\mathbb{Z}_n^*$ 中随机选取互不相同的 $s_1, s_2, \cdots, s_r$, 则 $s_1^2, s_2^2, \cdots, s_r^2$ 为随机的 r 个模 n 的二次剩余. 分别计算 $C(n, s_i^2)$ $(1 \leqslant i \leqslant r)$, 以 c 表示输出 1 的次数. 利用引理 3.3, 当 $r \geqslant 1/\delta\varepsilon^2$ 时, 有

$$\Pr\left(\left|\frac{c}{r} - \alpha\right| < \frac{\varepsilon}{2}\right) > 1 - \delta. \tag{3.3}$$

任取 $x \in \mathbb{Z}_n^1$, 令 $y_i = xs_i^2$. 当 x 为二次剩余时, $y_1, y_2, \cdots, y_r$ 为 r 个随机二次剩余. 分别计算 $C(n, y_i)$ $(1 \leqslant i \leqslant r)$, 以 $\overline{c}$ 表示输出为 1 的次数. 同样利用引理 3.3, 当 $r \geqslant 1/\delta\varepsilon^2$ 时, 有

$$\Pr\left(\left|\frac{\overline{c}}{r} - \alpha\right| < \frac{\varepsilon}{2} \,\middle|\, x\text{为二次剩余}\right) > 1 - \delta. \tag{3.4}$$

当 x 为非二次剩余时, $y_1, y_2, \cdots, y_r$ 为 r 个随机非二次剩余. 类似式 (3.4) 可得

$$\Pr\left(\left|\frac{\overline{c}}{r} - \beta\right| < \frac{\varepsilon}{2} \,\middle|\, x\text{为非二次剩余}\right) > 1 - \delta. \tag{3.5}$$

定义判断 x 是否为二次剩余的算法 $G(n,x)$ 如下:

若 $\left|\frac{c}{r} - \frac{\overline{c}}{r}\right| < \varepsilon$, 判定 x 为二次剩余, 令 $G(n,x)=1$;

若 $\left|\frac{c}{r} - \frac{\overline{c}}{r}\right| > \varepsilon$, 判定 x 为非二次剩余, 令 $G(n,x)=0$.

当 $\left|\frac{c}{r}-\alpha\right|<\frac{\varepsilon}{2}$ 和 $\left|\frac{\overline{c}}{r}-\alpha\right|<\frac{\varepsilon}{2}$ 同时成立时, 有

$$\left|\frac{c}{r}-\frac{\overline{c}}{r}\right|=\left|\frac{c}{r}-\alpha-\left(\frac{\overline{c}}{r}-\alpha\right)\right|<\left|\frac{c}{r}-\alpha\right|+\left|\frac{\overline{c}}{r}-\alpha\right|<\varepsilon.$$

利用式 (3.3) 和式 (3.4) 得

$$\begin{aligned}&\Pr\left(\left|\frac{c}{r}-\frac{\overline{c}}{r}\right|<\varepsilon\,\middle|\,x\text{为二次剩余}\right)\\ \geqslant&\Pr\left(\left|\frac{c}{r}-\alpha\right|<\frac{\varepsilon}{2}\right)\Pr\left(\left|\frac{\overline{c}}{r}-\alpha\right|<\frac{\varepsilon}{2}\,\middle|\,x\text{为二次剩余}\right)\\ >&(1-\delta)^2>1-2\delta.\end{aligned}$$

所以 $G(n,x)$ 正确判断 x 为二次剩余的概率大于 $1-\delta$ (不妨以 δ 代替 2δ).

当 $\left|\frac{c}{r}-\alpha\right|<\frac{\varepsilon}{2}$ 和 $\left|\frac{\overline{c}}{r}-\beta\right|<\frac{\varepsilon}{2}$ 同时成立时, 有 $\frac{c}{r}>\alpha-\frac{\varepsilon}{2}$ 及 $\frac{\overline{c}}{r}<\beta+\frac{\varepsilon}{2}$, 从而

$$\frac{c}{r}-\frac{\overline{c}}{r}>\alpha-\frac{\varepsilon}{2}-\left(\beta+\frac{\varepsilon}{2}\right)=\alpha-\beta-\varepsilon\geqslant\varepsilon.$$

利用式 (3.3) 和式 (3.5) 得

$$\begin{aligned}&\Pr\left(\left|\frac{c}{r}-\frac{\overline{c}}{r}\right|>\varepsilon\,\middle|\,x\text{为非二次剩余}\right)\\ \geqslant&\Pr\left(\left|\frac{c}{r}-\alpha\right|<\frac{\varepsilon}{2}\right)\Pr\left(\left|\frac{\overline{c}}{r}-\beta\right|<\frac{\varepsilon}{2}\,\middle|\,x\text{为非二次剩余}\right)\\ >&(1-\delta)^2>1-2\delta.\end{aligned}$$

所以 $G(n,x)$ 正确判断 x 为非二次剩余的概率也大于 $1-\delta$.

由弱大数定理, 取抽样次数 $r=P_1^2(k)P_2(k)$. 综合上述, 基于 $C(n,x)$ 构造了概率多项式时间算法 $G(n,x)$. 定理得证.

定理 3.14　给定多项式 P_1 和 P_2, 设 $k\in N'$. 假设对于 H_k 中至少 $1/P_1(k)$ 部分的 n, 函数 $C(n,x)$ 为 $Q_n(x)$ 的 $(1/P_2(k))$-逼近, 以 c_k 表示函数 C 的最小门数. 若二次剩余假设 (定义3.1) 成立, 则对任一多项式 $L(k)$, 当 k 足够大时有 $c_k>L(k)$ $\left(\text{即 } B=\bigcup\limits_{k\in N'}\{Q_n\,|\,n\in H_k\}\text{ 为不可逼近区分函数簇}\right)$.

证明　假设存在一个多项式 $L'(k)$ 及一无限自然数子集 $\overline{N}\subset N'$, 对所有的 $k\in\overline{N}$ 有 $c_k<L'(k)$ (即假设 B 不是不可逼近的). 对任一 $k\in\overline{N}$, 以 S_k 表示使 $C(n,x)$ 为 $Q_n(x)$ 的 $(1/P_2(k))$-逼近的那些 $n\in H_k$ 组成的子集, 则 $|S_k|\geqslant|H_k|/P_1(k)$. 以 $\overline{C}_k(n,x)$ 表示门数达到 c_k 的函数. 由定理 3.13, 基于函数 $\overline{C}_k(n,x)$ 构造的概率多

项式时间算法 $G(n,x)$, 对任一 $n \in S_k$ 和任一 $x \in \mathbb{Z}_n^1$, 以大于 $1-1/P_2(k)$ 的概率正确判断 x 是否为模 n 的二次剩余, P_2 可为任一多项式, 所以当差错概率足够小时, 对任一 x, $G(n,x)$ 都能正确判断它是否为模 n 的二次剩余. 由于 $\overline{C}_k(n,x)$ 的大小是多项式有界的, 易见 $G(n,x)$ 的大小也是多项式有界的, 这与二次剩余假设矛盾. 定理得证.

对于任一 $n = pq$, 若已知 n 的素因子 p 和 q, 则由定理 3.12, 存在复杂度为 $O(\lg^3(n))$ 的多项式时间算法, 能正确判断 $a \in \mathbb{Z}_n^1$ 是否为模 n 的二次剩余, 定理 3.14 中的 B 称为不可逼近的陷门区分函数簇.

定理 3.13 和定理 3.14 的证明可参考文献 [18] 中 6.3 节的定理 1 和推论 1.

习　题

习题 3.1　试证

$$\left(\frac{195}{1901}\right) = -1, \quad \left(\frac{74}{101}\right) = -1, \quad \left(\frac{365}{1847}\right) = 1.$$

习题 3.2　试证: 若 $p \equiv \pm 1 \text{或} \pm 5 \pmod{24}$, 则 $\left(\dfrac{6}{p}\right) = 1$;

若 $p \equiv \pm 7 \text{或} \pm 11 \pmod{24}$, 则 $\left(\dfrac{6}{p}\right) = -1$.

习题 3.3　写一个具体求 Legendre 符号的算法, 分析其复杂度.

习题 3.4　设素数 $p \nmid a$, 试证二次同余方程 $ax^2 + bx + c \equiv 0 \pmod{p}$ 的解的个数为 $1 + \left(\dfrac{b^2 - 4ac}{p}\right)$.

习题 3.5　设 $p \nmid a$, 证明 $\displaystyle\sum_{a=1}^{p-1} \left(\frac{ax+b}{p}\right) = 0$.

习题 3.6　证明

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1, & p \nmid a, \\ p-1, & p \mid a. \end{cases}$$

习题 3.7　证明 $1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

习题 3.8　令 Q 是模 p 的所有二次剩余的乘积, 试证

$$Q = \begin{cases} 1, & p \equiv 3 \pmod{4}, \\ -1, & p \equiv 1 \pmod{4}. \end{cases}$$

习题 3.9　证明

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1 \text{或} 3 \pmod{8}, \\ -1, & p \equiv 5 \text{或} 7 \pmod{8}. \end{cases}$$

第4章　特　　征

4.1　剩余系的表示

设 m 为一正整数, $A_0, A_1, \cdots, A_{m-1}$ 为 m 个剩余类, 它们组成一个加法群. 若将每个剩余类对应一个复数 (非零)

$$A_u \to \xi_u,$$

且具有下述性质: 当 $A_u + A_v = A_w$ 时, $\xi_u \cdot \xi_v = \xi_w$, 称此对应为剩余系的一个表示, 也就是剩余系加法群的一个表示.

取 $\xi_u = \mathrm{e}^{2\pi \mathrm{i} u/m}$, 就可以得到一个表示. 若 $u \equiv u' (\mathrm{mod}\ m)$, 则 $u = u' + km$,

$$\xi_u = \mathrm{e}^{2\pi\mathrm{i}(u'+km)/m} = \mathrm{e}^{2\pi\mathrm{i}u'/m} = \xi_{u'}.$$

若 $u + v \equiv w (\mathrm{mod}\ m)$, 则

$$\xi_u \cdot \xi_v = \mathrm{e}^{2\pi\mathrm{i}(u+v)/m} = \mathrm{e}^{2\pi\mathrm{i}w/m} = \xi_w,$$

所以 $A_u \to \xi_u$ 是一个表示. 设 a 为正整数, $1 \leqslant a \leqslant m$, 则 $A_u \to \xi_u^a = \mathrm{e}^{2\pi iau/m}$ 也是一个表示, 共得到 m 个不同的表示. 今证模 m 的剩余系也仅可能有 m 个表示, 设 $A_u \to \eta_u$ 为一个表示, 由于 $m \cdot A_1 = A_0$, 故 $\eta_1^m = 1$, η_1 是一个 m 次单位根. 设 $\eta_1 = \mathrm{e}^{2\pi\mathrm{i}a/m}$, 即 $\eta_1 = \xi_1^a$. 易见 $\eta_u = \eta_1^u = \xi_u^a$.

定理 4.1

$$\frac{1}{m}\sum_{a=0}^{m-1} \mathrm{e}^{2\pi\mathrm{i}an/m} = \begin{cases} 1, & m|n, \\ 0, & m \nmid n. \end{cases}$$

证明　若 $m|n$, 显然成立. 若 $m \nmid n$, 则

$$\sum_{a=0}^{m-1} \mathrm{e}^{2\pi\mathrm{i}an/m} = \frac{1 - (\mathrm{e}^{2\pi\mathrm{i}n/m})^m}{1 - \mathrm{e}^{2\pi\mathrm{i}n/m}} = 0.$$

设 $f(x_1, x_2, \cdots, x_n)$ 为整系数 n 个变量的多项式, 同余方程

$$f(x_1, x_2, \cdots, x_n) \equiv N\, (\mathrm{mod}\ m), \quad 0 \leqslant x_v \leqslant m-1$$

的解答数可表为

$$\frac{1}{m}\sum_{x_1=0}^{m-1}\cdots\sum_{x_n=0}^{m-1}\sum_{a=0}^{m-1}\mathrm{e}^{2\pi\mathrm{i}a(f(x_1,\cdots,x_n)-N)/m},$$

由此可见, 同余方程问题有了解析表达式.

4.2 特　　征

设 $a_1,a_2,\cdots,a_{\varphi(m)}$ 为小于 m 且与 m 互素的所有正整数, 剩余类 $A_{a_1},A_{a_2},\cdots,A_{a_{\varphi(m)}}$ 组成一个模 m 的缩系, 对乘法封闭, 组成一个乘法群. 考虑这个乘法群的表示, 称它的表示为特征.

定义 4.1　模 m 的特征 $\chi(m)$ 是一仅当 $(n,m)=1$ 时有定义的函数, 且适合:

(1) $\chi(1)\neq 0$;

(2) 若 $a\equiv b(\mathrm{mod}\ m)$, 则 $\chi(a)=\chi(b)$;

(3) $\chi(ab)=\chi(a)\chi(b)$.

有时为方便, 当 $(n,m)>1$ 时, 令 $\chi(n)=0$.

例 4.1　$\chi(n)$ 恒为 1, 显然是一个特征, 称为主特征, 记为 χ_0; $\chi(1)^2=\chi(1\cdot 1)=\chi(1)$, 因 $\chi(1)\neq 0$, 故 $\chi(1)=1$.

我们来找出模 m 的所有的特征, 首先考虑 $m=p$ 为一素数的特殊情况, 取 g 为模 p 的原根, 当 n 与 p 互素时, $n\equiv g^{\mathrm{ind}\,n}\,(\mathrm{mod}\ p)$, 函数

$$\chi_a(n)=\mathrm{e}^{2\pi\mathrm{i}a\,\mathrm{ind}\,n/(p-1)},\quad 1\leqslant a\leqslant p-1$$

具有下述性质:

(1) $\chi_a(1)=1(\mathrm{ind}\ 1=0)$;

(2) 若 $n\equiv n'(\mathrm{mod}\ p)$, 则 $\mathrm{ind}\ n\equiv \mathrm{ind}\ n'(\mathrm{mod}\ p-1)$, 故 $\chi_a(n)=\chi_a(n')$;

(3) $\chi_a(nn')=\mathrm{e}^{2\pi\mathrm{i}a\mathrm{ind}(nn')/p-1}=\mathrm{e}^{2\pi\mathrm{i}a(\mathrm{ind}n+\mathrm{ind}n')/p-1}=\chi_a(n)\chi_a(n')$,

所以 $\chi_a(n)$ 是一个特征. 当 $p\neq 2$ 时, 取 $a=\dfrac{p-1}{2}$, 则

$$\chi_{\frac{1}{2}(p-1)}(n)=\mathrm{e}^{\pi\mathrm{i}\mathrm{ind}\,n}=\left(\frac{n}{p}\right),$$

Legendre 符号是一个特征. 以上共得到了模 p 的 $p-1$ 个特征. 若 $\chi(n)$ 为模 p 的任一特征, 因为 $g^{p-1}\equiv 1\,(\mathrm{mod}\ p)$, 故 $\chi(g)^{p-1}=1$, $\chi(g)$ 为 $p-1$ 次单位根, 可能取 $p-1$ 个不同的值. 当 $\chi(g)$ 确定后, 所有的 $\chi(n)$ 也就确定了, 所以模 p 的特征共有 $p-1$ 个.

考虑一般的 m.

(1) $m=p^l$, p 是奇素数. 由定理 2.25, 存在模 p^l 的原根, 记为 g. 若 n 与 p 互素, 则 $n \equiv g^{\operatorname{ind} n} \pmod{p^l}$, 如此可得 $\varphi(p^l)$ 个特征

$$\chi_a(n)=\mathrm{e}^{2\pi \mathrm{i} a \operatorname{ind} n/\varphi(p^l)}, \quad 1 \leqslant a \leqslant \varphi(p^l).$$

当 $n \not\equiv 1 \pmod{p^l}$ 时,

$$\chi_1(n)=\mathrm{e}^{2\pi \mathrm{i}\cdot \operatorname{ind} n/\varphi(p^l)} \neq 1.$$

(2) $m=2^l$.

(a) $l=1$, 仅有一主特征.

(b) $l=2$, 除主特征之外, 还有一个特征: $\chi(1)=1, \chi(3)=-1$.

(c) $l>2$, 由定理 2.27, 当 n 为奇数时, 有一整数 b, 使

$$n \equiv (-1)^{\frac{1}{2}(n-1)} 5^b \pmod{2^l}, \quad b \geqslant 0.$$

定义

$$\chi_{a,c}(n)=(-1)^{\frac{1}{2}(n-1)a} \mathrm{e}^{2\pi \mathrm{i} c b/2^{l-2}},$$

其中 a 可取为 ± 1, c 可在 $[1,2^{l-2}]$ 之内, 故共有 $\varphi(2^l)=2^{l-1}$ 个特征. 特别地, 取

$$\chi_{1,1}(n)=(-1)^{\frac{1}{2}(n-1)} \mathrm{e}^{2\pi \mathrm{i} b/2^{l-2}},$$

若 $\chi_{1,1}(n)=1$, 则 $n \equiv 1 \pmod{2^l}$ 或 $n \equiv -5^{2^{l-3}} \pmod{2^l}$, 而当 $n \equiv -5^{2^{l-3}} \pmod{2^l}$ 时,

$$\chi_{0,1}(n)=-1,$$

即若 $n \not\equiv 1 \pmod{2^l}$ 时, 总存在一个特征 $\chi_{a,c}$, 使

$$\chi_{a,c}(n) \neq 1.$$

(3) 一般情况, 设 $m=p_1^{l_1} \cdots p_s^{l_s}$ 为标准因子分解式, 设 $\chi^v(n)$ 为模 $p_v^{l_v}$ 的一个特征, 则

$$\chi(n)=\prod_{v=1}^{s} \chi^v(n)$$

为模 m 的特征, 由此可得 $\varphi(m)$ 个模 m 的特征.

反之, 若特征 $\chi(n)$ 的模为

$$k=k_1 k_2 \cdots k_r,$$

此处 k_i 两两互素, 则存在以 $k_i (i=1,2,\cdots,r)$ 为模的特征 $\chi_i(n)$ 使

$$\chi(n)=\chi_1(n) \cdots \chi_r(n).$$

仅以 $r=2$ 为例证之. 对任一 n, 可定出 n_1 及 n_2 使

$$\begin{aligned}&n_1\equiv n\,(\mathrm{mod}\ k_1),\quad n_1\equiv 1\,(\mathrm{mod}\ k_2);\\&n_2\equiv 1\,(\mathrm{mod}\ k_1),\quad n_2\equiv n\,(\mathrm{mod}\ k_2).\end{aligned}$$

定义

$$\chi_1(n)=\chi(n_1),\quad \chi_2(n)=\chi(n_2),$$

可以证明 $\chi_1(n)$ 是 k_1 的特征, 同样 $\chi_2(n)$ 是模 k_2 的特征. 由 n_1 与 n_2 的定义可知

$$n_1n_2\equiv n\,(\mathrm{mod}\ k_1),\quad n_1n_2\equiv n\,(\mathrm{mod}\ k_2),$$

故 $n_1n_2\equiv n\,(\mathrm{mod}\ m)$, 即得

$$\chi(n)=\chi(n_1n_2)=\chi(n_1)\chi(n_2)=\chi_1(n)\chi_2(n).$$

定理 4.2 以上所造出的 $\varphi(m)$ 个特征互不相同.

证明 若

$$\prod_{v=1}^{s}\chi^{(v)}(n)=\prod_{v=1}^{s}\widetilde{\chi}^{(v)}(n),$$

欲证明对每个 v, $\chi^v=\widetilde{\chi}^{(v)}$, 因为 $\chi^{(v)}/\widetilde{\chi}^{(v)}$ 仍是模 $p_v^{l_v}$ 的特征, 故仅需证明, 若

$$\chi(n)=\prod_{v=1}^{s}\chi^{(v)}(n)$$

是主特征, 则每个 $\chi^{(v)}$ 都是模 $p_v^{l_v}$ 的主特征. 取

$$\begin{aligned}&n\equiv 1(\mathrm{mod}\ p_v^{l_v}),\quad 1\leqslant v\leqslant s-1,\\&n\equiv a(\mathrm{mod}\ p_s^{l_s}),\end{aligned}$$

这里 a 是可为任一与 p_s 互素的整数, 由 $\chi(n)=1$, 可得 $\chi^{(s)}(a)=1$, 即 $\chi^{(s)}$ 为模 $p_s^{l_s}$ 的主特征. 类似地可证, 对任一 v, $\chi^{(v)}$ 都是主特征.

定理 4.3 若 $n\not\equiv 1\,(\mathrm{mod}\ m)$, 则在这 $\varphi(m)$ 个特征中, 一定存在一个特征 χ, 使 $\chi(n)\neq 1$.

证明 由于 $n\not\equiv 1\,(\mathrm{mod}\ m)$, 一定存在一个 $p_v^{l_v}$, 使 $n\not\equiv 1\,(\mathrm{mod}\ p_v^{l_v})$, 取 $\chi^{(v)}$ 为模 $p_v^{l_v}$ 的一个特征, 且 $\chi^{(v)}(n)\neq 1$, 当 $u\neq v$ 时, 取 $\chi^{(u)}$ 为主特征, 令 $\chi=\prod\limits_{v=1}^{s}\chi^{(v)}$, 则 $\chi(n)\neq 1$, 即证.

定理 4.4

$$\sum_{n}\chi(n)=\begin{cases}\varphi(m), & \chi=\chi_0,\\ 0, & \chi\neq\chi_0,\end{cases}$$

求和号中 n 跑遍模 m 的完全剩余系.

证明 当 $\chi = \chi_0$ 时, 显然成立. 当 $\chi \neq \chi_0$ 时, 必有一整数 a, $(a, m) = 1$, 且 $\chi(a) \neq 1$, 由

$$\chi(a) \sum_n \chi(n) = \sum_n \chi(an) = \sum_n \chi(n),$$

即 $\big(\chi(a) - 1\big) \sum\limits_n \chi(n) = 0$, 故得定理.

定理 4.5 命 c 表示模 m 的特征总数, 则

$$\sum_\chi \chi(n) = \begin{cases} c, & n \equiv 1 \pmod{m}, \\ 0, & n \not\equiv 1 \pmod{m}. \end{cases}$$

证明 因 $n^{\varphi(m)} \equiv 1 \pmod{m}$, 故 $(\chi(n))^{\varphi(m)} = 1$, 特征个数总是有限的. 当 $n \equiv 1 \pmod{m}$ 时, 定理显然成立. 当 $n \not\equiv 1 \pmod{m}$ 时, 由定理 4.3, 一定存在一个特征 χ_1, 使 $\chi_1(n) \neq 1$, 由

$$\chi_1(n) \sum_\chi \chi(n) = \sum_\chi \chi_1 \chi(n) = \sum_\chi \chi(n)$$

可证得定理.

定理 4.6 模 m 的特征总数等于 $\varphi(m)$.

证明 由定理 4.4, 定理 4.5 知

$$\sum_{n,\chi} \chi(n) = \begin{cases} \displaystyle\sum_n \sum_\chi \chi(n) = c, \\ \displaystyle\sum_\chi \sum_n \chi(n) = \varphi(m), \end{cases}$$

故 $c = \varphi(m)$.

所以, 所造出的 $\varphi(m)$ 个模 m 的特征已包含了模 m 所有的特征. 令

$$\chi_1(n, 2^l) = (-1)^{\frac{(n-1)}{2}}, \quad \chi_2(n, 2^l) = \mathrm{e}^{2\pi \mathrm{i} b/2^{l-2}}, \quad \chi(n, p^l) = \mathrm{e}^{2\pi \mathrm{i} \,\mathrm{ind}\, n/\varphi(p^l)},$$

命 $m = 2^\alpha \prod p_v^{l_v}$, $2 \nmid p_v$, 模 m 的任一特征可分解为

$$\chi(n) = \begin{cases} \displaystyle\prod_\chi \chi(n, p_v^{l_v})^{c_v}, & a = 0, 1, \\ \displaystyle\chi_1(n, 2^l)^{c_0} \prod_v \chi(n, p_v^{l_v})^{c_v}, & a = 2, \\ \displaystyle\chi_1(n, 2^l)^{c_0} \chi_2(n, 2^l)^{c_0'} \prod_v \chi(n, p_v^{l_v})^{c_v}, & a \geqslant 3, \end{cases}$$

其中 $c_0 = 0, 1$, $1 \leqslant c_0' < 2^{l-2}$, $0 \leqslant c_v < \varphi(p_v^{l_v})$.

4.3 原 特 征

设 χ 为模 m 的特征, 若存在 m 的一个真因子 M $(m \neq M)$, 具有下述性质: 当

$$n \equiv n'(\bmod M), \quad (n,m)=1, \quad (n',m)=1$$

时, $\chi(n)=\chi(n')$, 称 χ 为模 m 的非原特征, 否则称为模 m 的原特征.

当 $m \neq 1$ 时, 主特征是非原特征 (可取 $M=1$).

当 $m=p$ 为素数时, 非主特征都是原特征.

当 $m=p^l$ $(2 \nmid p, l>1)$ 时, 特征

$$\chi_a(n)=\mathrm{e}^{2\pi\mathrm{i} a \operatorname{ind} n/\varphi(p^l)}$$

为原特征的必要充分条件是 $p \nmid a$ (因为模 p^l 的非原特征一定诱导出一个模 p^{l-1} 的特征).

若 $m=2^l, l=1$, 仅有主特征, $l=2$ 时, 非主特征 $\chi(1)=1, \chi(3)=-1$ 是原特征.

当 $l \geqslant 3$ 时, 若 $\chi_{a,c}(n)=\chi_{a,c}(n+2^{l-1})$(反之亦真), 即

$$(-1)^{\frac{n-1}{2}a}\mathrm{e}^{2\pi\mathrm{i}cb/2^{l-2}}=(-1)^{\frac{1}{2}a(n-1+2^{l-1})}\mathrm{e}^{2\pi\mathrm{i}cb'/2^{l-2}}=(-1)^{\frac{n-1}{2}a}\mathrm{e}^{2\pi\mathrm{i}cb'/2^{l-2}},$$

因而 $c(b-b') \equiv 0\,(\bmod 2^{l-2})$, 这里 $n+2^{l-1} \equiv (-1)^{\frac{n-1}{2}} \cdot 5^{b'}\,(\bmod 2^{l'})$. 由于

$$\begin{aligned} n+2^{l-1} &\equiv n+n\cdot 2^{l-1}(\bmod 2^l) \\ &\equiv n(1+2^{l-1})(\bmod 2^l) \\ &\equiv n\cdot 5^{2^{l-3}}(\bmod 2^l), \end{aligned}$$

故

$$b' \equiv b+2^{l-3}\,(\bmod 2^{l-2}),$$

可见 $\chi_{a,c}$ 为原特征的充分必要条件为 $2 \nmid c$.

例 4.2 取 $m=8$(即 $l=3$),

$$\chi_{a,c}(n)=(-1)^{\frac{n-1}{2}a+cb}.$$

当 $n=1,3,5,7$ 时, $b=0,1,1,0$. 当 $c=1$ 时,

$$\chi_{a,1}(1)=1, \quad \chi_{a,1}(3)=-(-1)^a, \quad \chi_{a,1}(5)=-1, \quad \chi_{a,1}(7)=(-1)^a$$

是原特征, 实际上, $\chi_{0,1}(n)=\left(\dfrac{2}{n}\right), \chi_{1,1}=\left(\dfrac{-2}{n}\right)$, 而 $c=0$ 时,

$$\chi_{1,0}=1,\quad \chi_{1,0}(3)=-1,\quad \chi_{1,0}(5)=1,\quad \chi_{1,0}(7)=-1,$$

即 $\chi_{1,0}(n)=\left(\dfrac{-1}{n}\right)$, 它是模 4 的特征, 所以不是模 8 的原特征.

一般地, 若利用 4.2 节的表示法

$$\chi(n)=\prod_{v}\chi^{(v)}(n),$$

当 $\chi^{(v)}$ 中有一个为模 $p_v^{l_v}$ 的非原特征时, χ 为模 m 的非原特征. 反之, 若 χ 是模 m 的非原特征, 则一定有一个 $\chi^{(v)}$ 是模 $p_v^{l_v}$ 的非原特征.

考虑取实数值的原特征, 当 p 为奇素数时, 若 $\chi(n,p^l)^{c_v}=\mathrm{e}^{2\pi\mathrm{i}c_v\cdot\mathrm{ind}\,n/\varphi(p^l)}$, 总取实值, 则 c_v 是 $\varphi(p^l)/2$ 的倍数, 由上述, 当 $p\nmid c_v$ 时为原特征, 故仅当 $l=1, c_v=(p-1)/2$ 时, 它为实原特征.

设 $\chi(n,2^l)^{c_0}=\mathrm{e}^{2\pi\mathrm{i}c_0b/2^{l-2}}$ 为实原特征, 则必有 $2^{l-3}|c_0$, c_0 又是奇数, 故 $l\leqslant 3$.

设 $m=2m', 2\nmid m'$, 这时模 m 的特征也是模 m' 的特征, 不存在模 m 的原特征.

综合上述, 仅当 $m=2^a p_1\cdots p_s,\ a=0,2,3$ 时, 有实原特征. 因 $c_v=\dfrac{1}{2}\varphi(p)$, 故

$$\chi(n,p_v)^{\frac{1}{2}(p-1)}=\mathrm{e}^{\pi\mathrm{i}\,\mathrm{ind}\,n}=\left(\frac{n}{p}\right).$$

当 $a=0$ 时, 该实原特征就是 Jacobi 符号

$$\left(\frac{n}{m}\right),\quad (n,m)=1;$$

当 $a=2$ 时, 实原特征就是

$$(-1)^{\frac{1}{2}(n-1)}\left(\frac{n}{m/4}\right),\quad (n,m)=1;$$

当 $a=3$ 时, 有两个实原特征

$$\left(\frac{2}{n}\right)\left(\frac{n}{m/8}\right),\quad (n,m)=1;$$

以及

$$\left(\frac{-2}{n}\right)\left(\frac{n}{m/8}\right),\quad (n,m)=1.$$

4.4 特 征 和

命特征和

$$s(a,\chi)=\sum_{n=1}^{m}\chi(n)\mathrm{e}^{2\pi \mathrm{i}an/m}.$$

定理 4.7 设 $m=m_1m_2,(m_1,m_2)=1$ 且 $\chi(n)=\chi_1(n)\chi_2(n)$, 这里 χ_1 是模 m_1 的特征, χ_2 是模 m_2 的特征, 则

$$s(a,\chi)=\chi_1(m_2)\chi_2(m_1)s(a,\chi_1)s(a,\chi_2).$$

证明 令 $n=m_1n_2+m_2n_1$, 当 n_1,n_2 分别跑遍模 m_1,m_2 的完全剩余系时, n 则跑遍模 m 的完全剩余系, 故

$$\begin{aligned}s(a,\chi)&=\sum_{n_1=1}^{m_1}\sum_{n_2=1}^{m_2}\chi_1(m_1n_2+m_2n_1)\chi_2(m_1n_2+m_2n_1)\mathrm{e}^{2\pi \mathrm{i}a(m_1n_2+m_2n_1)/m_1m_2}\\&=\sum_{n_1=1}^{m_1}\chi_1(m_2n_1)\mathrm{e}^{2\pi \mathrm{i}an_1/m_1}\sum_{n_2=1}^{m_2}\chi_2(m_1n_2)\mathrm{e}^{2\pi \mathrm{i}an_2/m_2}\\&=\chi_1(m_2)\chi_2(m_1)s(a,\chi_1)s(a,\chi_2).\end{aligned}$$

由定理 4.7 可知, 仅需研究以素数幂为模之特征和.

定理 4.8 令 $m=p^l$. 若 $p|a$ 及 χ 为原特征, 或若 $p\nmid a$ 及 χ 是非原特征 (但若 $l=1$, 则 $\chi=\chi_0$ 的情况应除外), 则 $s(a,\chi)=0$.

证明 令 $n=x(1+p^{l-1}y)$, 当 x 过模 p^{l-1} 的缩剩余系, y 过模 p 的完全剩余系时, n 过模 p^l 的缩系, 故

$$s(a,\chi)=\sum_{x=1}^{p^{l-1}}\chi(x)\mathrm{e}^{2\pi \mathrm{i}ax/p^l}\sum_{y=1}^{p}\chi(1+p^{l-1}y)\mathrm{e}^{2\pi \mathrm{i}axy/p}.$$

若 χ 为非原特征, 这时 $l>1$, 故 $\chi(1+p^{l-1}y)=1$, 这时

$$s(a,\chi)=\begin{cases}0, & p\nmid a,\\ p\displaystyle\sum_{x=1}^{p^{l-1}}\chi(x)\mathrm{e}^{2\pi \mathrm{i}ax/p^l}, & p|a.\end{cases}$$

若 χ 为原特征, 则一定有一 u, 使 $\chi(1+p^{l-1}u)\neq 1$, 由于 $p|a$, 而当 $l>1$ 时, 有

$$\chi(1+p^{l-1}u)\sum_{y=1}^{p}\chi(1+p^{l-1}y)=\sum_{y=1}^{p}\chi(1+p^{l-1}(y+u))=\sum_{y=1}^{p}\chi(1+p^{l-1}y),$$

故 $\sum_{y=1}^{p}\chi(1+p^{l-1}y)=0$, 当 $l=1$ 时, 由定理 4.4 可知, 定理当 $\chi\neq\chi_0$ 时也成立, 证毕.

记

$$\tau(\chi)=s(1,\chi).$$

若 $(a,m)=1$, 则

$$\chi(a)\cdot s(a,\chi)=\sum_{n=1}^{m}\chi(an)\mathrm{e}^{2\pi \mathrm{i}an/m}=s(1,\chi).$$

若能计算 $s(1,\chi)$, 就能得到 $s(a,\chi)$ $((a,m)=1)$.

定理 4.9　令

$$C_q(n)=\sum_{(a,q)=1}\mathrm{e}^{2\pi \mathrm{i}an/q},$$

其中 a 跑遍模 q 之缩系, 则

(1) 当 $(q_1,q_2)=1$ 时, $C_{q_1q_2}(n)=C_{q_1}(n)C_{q_2}(n)$;

(2)
$$C_{p^l}(n)=\begin{cases}p^l-p^{l-1}, & p^l|n,\\ -p^{l-1}, & p^l\nmid n,p^{l-1}|n,\\ 0, & p^{l-1}\nmid n;\end{cases}$$

(3) $C_q(1)=\mu(q)$(当 q 有重因子时为零, 当 q 无重因子时, $\mu(q)=(-1)^r,r$ 为 q 的素因子个数).

证明　(1) 令 $q=q_1a_2+q_2a_1,a_1,a_2$ 分别跑遍模 q_1,q_2 的缩系, 代入即证.

(2)
$$C_{p^l}(n)=\sum_{a=1}^{p^l}\mathrm{e}^{2\pi \mathrm{i}an/p^l}-\sum_{a=1}^{p^{l-1}}\mathrm{e}^{2\pi \mathrm{i}an/p^{l-1}},$$

利用定理 4.1, 即可证.

(3) 由 (1) 和 (2) 即可推得.

定理 4.10　若 χ 是原特征, 则

$$|\tau(\chi)|^2=m.$$

证明 由定理 4.7, 仅需讨论 $m=p^l$ 之特例.

$$
\begin{aligned}
|\tau(\chi)|^2 &= \tau(\chi)\overline{\tau}(\chi) \\
&= \sum_{n=1}^{p^l}\chi(n)\mathrm{e}^{2\pi\mathrm{i}n/p^l}\sum_{q=1}^{p^l}\overline{\chi}(q)\mathrm{e}^{-2\pi\mathrm{i}q/p^l} \\
&= \sum_{n=1}^{p^l}\chi(n)\mathrm{e}^{2\pi\mathrm{i}n/p^l}\sum_{q=1}^{p^l}\overline{\chi}(nq)\mathrm{e}^{-2\pi\mathrm{i}nq/p^l} \\
&= \sum_{q=1}^{p^l}\overline{\chi}(q)\sum_{n=1,(p,n)=1}^{p^l}\mathrm{e}^{2\pi\mathrm{i}(1-q)n/p^l},
\end{aligned}
$$

若 $p^{l-1}\nmid q-1$, 由定理 4.9 可知, 上式右边对应的内和为零, 故假设 $p^{l-1}|q-1$, 即

$$
q-1=p^{l-1}u, \quad 0\leqslant u\leqslant p-1,
$$

则有

$$
\begin{aligned}
|\tau(\chi)|^2 &= p^l-p^{l-1}+\sum_{u=1}^{p-1}\overline{\chi}(1+p^{l-1}u)\sum_{n=1,(p,n)=1}^{p^l}\mathrm{e}^{-2\pi\mathrm{i}un/p} \\
&= p^l-p^{l-1}-p^{l-1}\sum_{u=1}^{p-1}\overline{\chi}(1+p^{l-1}u) \\
&= p^l-\sum_{u=1}^{p}\overline{\chi}(1+p^{l-1}u),
\end{aligned}
$$

由于 χ 为原特征, 类似于定理 4.8 的证明, 可知上式中的和为零, 故证得定理.

故有

$$
\tau(\chi)=\epsilon\sqrt{m}, \quad |\epsilon|=1,
$$

但要确定 ϵ, 并非易事.

定理 4.11 若 χ 是实原特征, m 为奇数, 有

$$
\tau(\chi)=\begin{cases}\pm\sqrt{m}, & m\equiv 1\,(\mathrm{mod}\ 4), \\ \pm\mathrm{i}\sqrt{m}, & m\equiv 3\,(\mathrm{mod}\ 4).\end{cases}
$$

证明　由 4.3 节的讨论, 可知 m 无平方因子. 设 $m=p$ 为素数,

$$\begin{aligned}\tau(\chi)^2 &= \sum_{n=1}^{p-1}\chi(n)\mathrm{e}^{2\pi\mathrm{i}n/p}\cdot\sum_{q=1}^{p-1}\chi(q)\mathrm{e}^{2\pi\mathrm{i}q/p}\\ &= \sum_{n=1}^{p-1}\chi(n)\mathrm{e}^{2\pi\mathrm{i}n/p}\sum_{q=1}^{p-1}\chi(nq)\mathrm{e}^{2\pi\mathrm{i}nq/p}\\ &= \sum_{q=1}^{p-1}\chi(q)\sum_{n=1}^{p-1}\mathrm{e}^{2\pi\mathrm{i}n(1+q)/p}\\ &= \chi(-1)(p-1)+\sum_{q=1}^{p-2}\chi(q)\cdot(-1)\\ &= \chi(-1)(p-1)+(-\chi(-1))(-1)\\ &= \chi(-1)p,\end{aligned}$$

而

$$\chi(-1)=\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},$$

易见这时定理成立, 由此可推出当 m 为几个奇素数之积时, 定理也成立.

4.5　Gauss 和

三角和

$$s(n,m)=\sum_{x=1}^{m}\mathrm{e}^{2\pi\mathrm{i}x^2n/m},\quad (n,m)=1$$

称为 Gauss 和.

定理 4.12　若 $(m,m')=1$, 则

$$s(n,mm')=s(nm',m)s(nm,m').$$

证明　令 $x=my+m'z$, 则

$$\begin{aligned}s(n,mm') &= \sum_{x=1}^{m}\mathrm{e}^{2\pi\mathrm{i}x^2n/mm'}=\sum_{y=1}^{m'}\sum_{z=1}^{m}\mathrm{e}^{2\pi\mathrm{i}(my+m'z)^2n/mm'}\\ &= \sum_{y=1}^{m'}\mathrm{e}^{2\pi\mathrm{i}y^2mn/m'}\sum_{z=1}^{m}\mathrm{e}^{2\pi\mathrm{i}z^2m'n/m}=s(nm',m)s(nm,m').\end{aligned}$$

由此可知, 仅需计算 $s(n,p^l)$ (p 为素数).

定理 4.13 令

$$\delta = \begin{cases} 1, & p \text{ 为奇素数}, \\ 2, & p = 2, \end{cases}$$

则当 $l \geqslant 2\delta$ 时,

$$s(n, p^l) = ps(n, p^{l-2}).$$

证明 令 $x = y + p^{l-\delta}z$. 由于 $2(l-\delta) \geqslant l$, 则有

$$\begin{aligned} s(n, p^l) &= \sum_{y=1}^{p^{l-\delta}} \sum_{z=1}^{p^\delta} \mathrm{e}^{2\pi\mathrm{i}(y+p^{l-\delta}z)^2 n/p^l} \\ &= \sum_{y=1}^{p^{l-\delta}} \mathrm{e}^{2\pi\mathrm{i}y^2 n/p^l} \cdot \sum_{z=1}^{p^\delta} \mathrm{e}^{4\pi\mathrm{i}yzn/p^\delta} \\ &= p^\delta \sum_{y=1}^{p^{l-\delta-1}} \mathrm{e}^{2\pi\mathrm{i}y^2 n/p^{l-2}}. \end{aligned}$$

当 $p > 2$ 时, 即为所求, 当 $p = 2$ 时, 由于

$$p \sum_{y=1}^{p^{l-3}} \mathrm{e}^{2\pi\mathrm{i}y^2 n/p^{l-2}} = \sum_{y=1}^{p^{l-2}} \mathrm{e}^{2\pi\mathrm{i}y^2 n/p^{l-2}},$$

亦得所求.

由上述讨论, 仅需研究下述 Gauss 和

$$s(n, 2), \quad s(n, 4), \quad s(n, 8), \quad s(n, p), \quad p\text{为奇素数}.$$

定理 4.14 若 $2 \nmid n$, 则

$$s(n, 2) = 0, \quad s(n, 4) = 2(1 + \mathrm{i}^n), \quad s(n, 8) = 4\mathrm{e}^{\pi\mathrm{i}\frac{n}{4}}.$$

证明 $s(n, 2) = 1 + \mathrm{e}^{2\pi\frac{\mathrm{i}}{2}} = 1 - 1 = 0$;

$$s(n, 4) = 1 + \mathrm{e}^{\frac{2\pi\mathrm{i}}{4}n} + \mathrm{e}^{\frac{2\pi\mathrm{i}}{4}4n} + \mathrm{e}^{\frac{2\pi\mathrm{i}}{4}\cdot 9n} = 1 + \mathrm{i}^n + 1 + \mathrm{i}^n = 2(1 + \mathrm{i}^n);$$
$$s(n, 8) = 2(1 + \mathrm{e}^{\frac{2\pi\mathrm{i}}{8}\cdot n} + \mathrm{e}^{\frac{2\pi\mathrm{i}}{8}\cdot 4n} + \mathrm{e}^{\frac{2\pi\mathrm{i}}{8}\cdot 9n}) = 4\mathrm{e}^{\frac{\pi\mathrm{i}}{4}n}.$$

定理 4.15 若 p 为奇素数, 则

$$s(n, p) = \left(\frac{n}{p}\right) s(1, p) = \left(\frac{n}{p}\right) \tau(\chi),$$

其中 $\chi(a) = \left(\dfrac{a}{p}\right)$.

证明 方程 $x^2 \equiv u\,(\mathrm{mod}\ p)$ 的解数为 $1+\left(\dfrac{u}{p}\right)$, 故

$$s(n,p)=\sum_{x=1}^{p}\mathrm{e}^{2\pi\mathrm{i}x^2n/p}=\sum_{u=1}^{p}\left(1+\left(\frac{u}{p}\right)\right)\mathrm{e}^{2\pi\mathrm{i}un/p}$$
$$=\sum_{u=1}^{p}\left(\frac{u}{p}\right)\mathrm{e}^{2\pi\mathrm{i}un/p}=\left(\frac{n}{p}\right)\sum_{v=1}^{p}\left(\frac{v}{p}\right)\mathrm{e}^{2\pi\mathrm{i}v/p}.$$

定理 4.16

$$s(1,p)=\sum_{v=1}^{p}\left(\frac{v}{p}\right)\mathrm{e}^{2\pi\mathrm{i}v/p}=\begin{cases}\sqrt{p}, & p\equiv 1\,(\mathrm{mod}\ 4),\\ \mathrm{i}\sqrt{p}, & p\equiv 3\,(\mathrm{mod}\ 4).\end{cases}$$

证明从略.

习 题

习题 4.1 (Fermat 问题) 当 $k\geqslant 3$ 时, 不定方程 $x^k+y^k=z^k$ 无整数解. 试证 Fermat 问题即为求证:

$$\int_0^1\left(\sum_{x=1}^{N}\mathrm{e}^{2\pi\mathrm{i}x^k\alpha}\right)^2\left(\sum_{x=1}^{N}\mathrm{e}^{-2\pi\mathrm{i}x^k\alpha}\right)\mathrm{d}\alpha=0.$$

习题 4.2 (Goldbach 问题) 任一偶数 ($\geqslant 2$) 可表为两个素数之和. 试证 Goldbach 问题即为求证:

$$\int_0^1\left(\sum_{p\leqslant 2N}\mathrm{e}^{2\pi\mathrm{i}p\alpha}\right)^2\mathrm{e}^{-4\pi\mathrm{i}N\alpha}\mathrm{d}\alpha>0,$$

其中求和号中的 p 跑遍 $\leqslant 2N$ 的素数.

习题 4.3 设 $(n,m)=1$,

$$S=\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\xi(x)\eta(y)\mathrm{e}^{2\pi\mathrm{i}xyn/m},\quad \sum_{x=0}^{m-1}|\xi(x)|^2=X_0,\quad \sum_{y=0}^{m-1}|\eta(y)|^2=Y_0,$$

试证

$$|S|\leqslant\sqrt{X_0Y_0m}.$$

第 5 章　连　分　数

5.1　简单连分数

分数

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots+\cfrac{1}{a_N}}}}$$

称为有限连分数. 当 $N=\infty$ 时, 称为连分数. 下面证明连分数确实是一个数, 为了书写方便, 上述分数常以

$$[a_0,a_1,a_2,\cdots,a_N]$$

表示, 易见

$$[a_0]=\frac{a_0}{1},\quad [a_0,a_1]=\frac{a_0a_1+1}{a_1},\quad [a_0,a_1,a_2]=\frac{a_2a_1a_0+a_2+a_0}{a_2a_1+1}.$$

通常写

$$[a_0,a_1,\cdots,a_n]=\frac{p_n}{q_n},\quad 0\leqslant n\leqslant N,$$

p_n,q_n 为 $a_0,a_1,\cdots,a_n$ 的多项式, $\dfrac{p_n}{q_n}$ 称为 $[a_0,a_1,\cdots,a_N]$ 的第 n 个渐近分数.

定理 5.1　渐近分数间有关系

$$\begin{aligned}&p_0=a_0,\quad p_1=a_1a_0+1,\quad p_n=a_np_{n-1}+p_{n-2}\quad (2\leqslant n\leqslant N);\\&q_0=1,\quad q_1=a_1,\quad q_n=a_nq_{n-1}+q_{n-2}\quad (2\leqslant n\leqslant N).\end{aligned}$$

证明　$n=0,1,2$ 时可直接验证, 今用归纳法, 设

$$[a_0,a_2,\cdots,a_m]=\frac{p_m}{q_m}=\frac{a_mp_{m-1}+p_{m-2}}{a_mq_{m-1}+q_{m-2}},$$

则

$$\begin{aligned}\frac{p_{m+1}}{q_{m+1}} &= [a_0, a_1, \cdots, a_m, a_{m+1}] = \left[a_0, a_1, \cdots, a_m + \frac{1}{a_{m+1}}\right] \\ &= \frac{\left(a_m + \dfrac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \dfrac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} = \frac{a_{m+1}\left(a_m p_{m-1} + p_{m-2}\right) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} \\ &= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}},\end{aligned}$$

即证.

定理 5.2 p_n 与 q_n 适合

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}, \quad n \geqslant 1, \tag{5.1}$$

即

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}};$$

以及

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n, \quad n \geqslant 2. \tag{5.2}$$

证明 $n = 1$ 时, 式 (5.1) 显然成立. 利用归纳法及定理 5.1 知

$$\begin{aligned}p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^{n-1}.\end{aligned}$$

又由定理 5.1 及式 (5.1) 可得

$$\begin{aligned}p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^n a_n,\end{aligned}$$

证毕.

若 a_0 为整数, $a_1, a_2, \cdots$ 为正整数, 则

$$[a_0, a_1, a_2, \cdots]$$

称为简单连分数, 本章中仅讨论简单连分数, 由定理 5.1 及定理 5.2 易得如下结论.

定理 5.3 对于简单连分数, 则有

(1) 当 $n > 1$, 则 $q_n \geqslant q_{n-1} + 1$, 故 $q_n \geqslant n$;

(2) $\dfrac{p_{2n+1}}{q_{2n+1}} < \dfrac{p_{2n-1}}{q_{2n-1}}, \quad \dfrac{p_{2n}}{q_{2n}} > \dfrac{p_{2n-2}}{q_{2n-2}}$;

(3) p_n/q_n 为既约分数.

证明 (1) 显然, 由定理 5.2 的式 (5.2) 可证 (2), 由式 (5.1) 可推得 (3), 证毕.

5.2 用连分数表实数

令 α 为一实数, 可以通过下述方法得到一个连分数. 取 $a_0=[\alpha]$, 令

$$\alpha_1'=\frac{1}{\alpha-[\alpha]},\quad a_1=[\alpha_1'];$$

再令

$$\alpha_2'=\frac{1}{\alpha_1'-[\alpha_1']},\quad a_2=[\alpha_2'];$$

继续此法, 令

$$\alpha_n'=\frac{1}{\alpha_{n-1}'-[\alpha_{n-1}']},\quad a_n=[\alpha_n'].$$

如此, 得到连分数 $[a_0,a_1,a_2,\cdots]$, 现在要考虑的是此连分数与 α 有何关系, 在讨论这个问题之前, 先来看一个特例.

设 $\alpha=\dfrac{p}{q}$ 为有理数, 由于 $a_0=\left[\dfrac{p}{q}\right]$, 所以 $p=a_0q+r_1(0\leqslant r_1<q)$, 而 $\alpha_1'=\left(\dfrac{p}{q}-a_0\right)^{-1}=\dfrac{q}{r_1}$, 同样地, $q=a_1r_1+r_2(0\leqslant r_2<r_1)$, $\alpha_2'=\dfrac{r_1}{r_2}$. 依此类推, 所以求 α 所对应的连分数的过程实际上与辗转相除法一致且

$$\alpha=[a_0,\alpha_1']=[a_0,a_1,\alpha_2']=\cdots=[a_0,a_1,\cdots,a_N],$$

α 可表为有限连分数.

回到一般情况, 设 α 为任一实数, 按上述方法求得其对应的连分数为 $[a_0,a_1,a_2,\cdots]$, 这是一个简单连分数, 以 $\alpha_n=[a_0,a_1,\cdots,a_n]$ 表示其第 n 个渐近分数, 由定理 5.2 可知

$$\alpha_0<\alpha_2<\alpha_4<\cdots<\alpha_{2n}<\cdots,$$
$$\alpha_1>\alpha_3>\alpha_5>\cdots>\alpha_{2n+1}>\cdots,$$

而

$$\alpha_1>\alpha_{2n+1}>\alpha_{2n}>\alpha_0,$$

可见递减序列 $\{\alpha_{2n+1}\}$ 与递增序列 $\{\alpha_{2n}\}$ 都有极限. 又由于

$$|\alpha_{2n+1}-\alpha_{2n}|=\left|\frac{p_{2n+1}}{q_{2n+1}}-\frac{p_{2n}}{q_{2n}}\right|=\frac{1}{q_{2n}q_{2n+1}}\leqslant\frac{1}{2n(2n+1)}\to 0,$$

故

$$\lim_{n\to\infty}\alpha_{2n+1}=\lim_{n\to\infty}\alpha_{2n}.$$

这里, 实际上证明了任一简单连分数的渐近分数都收敛于一个实数. 进一步地, 将证明此极限就是 α(当 $a_1, a_2, \cdots$ 为正数时, 由上述推论可知, $[a_0, a_1, a_2, \cdots]$ 的渐近分数也是收敛的).

定理 5.4 设 α 为任一实数, 则有

$$q_n\alpha - p_n = \frac{(-1)^n\delta_n}{q_{n+1}}, \quad 0 < \delta_n < 1$$

(若 α 为有理数, 此式仅当 $1 \leqslant n \leqslant N-2$ 时成立, 而 $\delta_{N-1} = 1$) 且 δ_n/q_{n+1} 为一递减序列.

证明 我们有

$$\alpha = [a_0, \alpha_1'] = [a_0, a_1, \alpha_2'] = \cdots = [a_0, a_1, \cdots, \alpha_n'] = \cdots,$$

由于

$$\frac{p_n}{q_n} = [a_0, a_1, \cdots, a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}},$$

故

$$\alpha = \left[a_0, a_1, \cdots, a_n + \frac{1}{\alpha_{n+1}'}\right] = \frac{\left(a_n + \dfrac{1}{\alpha_{n+1}'}\right)p_{n-1} + p_{n-2}}{\left(a_n + \dfrac{1}{\alpha_{n+1}'}\right)q_{n-1} + q_{n-2}}$$

$$= \frac{\alpha_{n+1}'(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{\alpha_{n+1}'(a_n q_{n-1} + q_{n-2}) + q_{n-1}} = \frac{\alpha_{n+1}' p_n + p_{n-1}}{\alpha_{n+1}' q_n + q_{n-1}},$$

因而

$$\alpha - \frac{p_n}{q_n} = \frac{q_n p_{n-1} - q_{n-1} p_n}{q_n(\alpha_{n+1}' q_n + q_{n-1})} = \frac{(-1)^n}{q_n(\alpha_{n+1}' q_n + q_{n-1})}.$$

故

$$\delta_n = \frac{q_{n+1}}{\alpha_{n+1}' q_n + q_{n-1}} = \frac{a_{n+1} q_n + q_{n-1}}{\alpha_{n+1}' q_n + q_{n-1}},$$

所以除了 $a_{n+1} = \alpha_{n+1}'$, 皆有 $0 < \delta_n < 1$, 又因 $\alpha_n' = a_n + \dfrac{1}{\alpha_{n+1}'}$, 可知

$$\frac{\delta_n}{q_{n+1}} = \frac{1}{\alpha_{n+1}' q_n + q_{n-1}} \geqslant \frac{1}{(a_{n+1}+1)q_n + q_{n-1}} = \frac{1}{q_{n+1} + q_n}$$

$$\geqslant \frac{1}{a_{n+2} q_{n+1} + q_n} = \frac{1}{q_{n+2}} \geqslant \frac{\delta_{n+1}}{q_{n+2}},$$

证毕.

由定理 5.4, 立即推出如下定理.

定理 5.5 若 α 为无理数, 则

$$\lim_{n\to\infty}\frac{p_n}{q_n}=\alpha.$$

定理 5.6

$$\left|\alpha-\frac{p_n}{q_n}\right|\leqslant\frac{1}{q_nq_{n+1}}<\frac{1}{q_n^2}.$$

例 5.1 试将 $\sqrt{3}$ 表为连分数.

$$a_0=[\sqrt{3}]=1,\quad \alpha_1'=\frac{1}{\sqrt{3}-1}=\frac{\sqrt{3}+1}{2},\quad a_1=[\alpha_1']=1,$$
$$\alpha_2'=\frac{2}{\sqrt{3}-1}=\sqrt{3}+1,\quad a_2=2,\quad \alpha_3'=\frac{1}{\sqrt{3}-1}=\alpha_1',$$

所以 $\sqrt{3}=[1,1,2,1,2,\cdots]$, 称此类连分数为循环连分数, 可以证明, α 可表为循环连分数的充分必要条件是 α 适合一个整系数的二次不可约多项式.

$\sqrt{3}$ 最初的几个渐近分数为 $\dfrac{1}{1},\dfrac{2}{1},\dfrac{5}{3},\dfrac{7}{4},\dfrac{19}{11},\dfrac{26}{15},\dfrac{71}{41},\dfrac{97}{56},\cdots$.

5.3 最佳渐近分数

在分母不超过 M 的所有分数中, 与 α 最接近的分数称为 α 的最佳渐近分数. 由 α 的连分数展开式所得到的渐近分数都是最佳渐近分数. 具体地说, 有如下定理.

定理 5.7 设 $n\geqslant 1, 0<q\leqslant q_n$, 且 $p/q\neq p_n/q_n$, 则

$$\left|\frac{p_n}{q_n}-\alpha\right|<\left|\frac{p}{q}-\alpha\right|,$$

故在分母不大于 q_n 的分数中, p_n/q_n 与 α 最接近.

证明 若能证明

$$|p_n-\alpha q_n|<|p-\alpha q|,$$

则定理已明. 由定理 5.4 知, $|p_n-\alpha q_n|$ 是递减序列.

(1) 若 $\alpha=[\alpha]+\dfrac{1}{2}$, 则 $\dfrac{p_1}{q_1}=\alpha$, 定理当 $n=1$ 时成立;

(2) 若 $\alpha<[\alpha]+\dfrac{1}{2}$, 则 $\dfrac{p_0}{q_0}=[\alpha]$, $[\alpha]$ 是离 α 最近的整数, $q_0=1$, 故定理当 $n=0$ 时成立;

(3) 若 $\alpha>[\alpha]+\dfrac{1}{2}$, 则 $1<\dfrac{1}{\alpha-[\alpha]}<2$, 故 $a_1=1$, $\dfrac{p_1}{q_1}=[\alpha]+1$, $q_1=1$, $\dfrac{p_1}{q_1}$ 是

离 α 最近的整数, 故定理当 $n=1$ 时成立.

归纳假设, 当 $0<q\leqslant q_{n-1}$, $p/q\neq p_{n-1}/q_{n-1}$ 时, 有

$$|p_{n-1}-\alpha q_{n-1}|<|p-\alpha q|,$$

由于 $|p_n-\alpha q_n|<|p_{n-1}-\alpha q_{n-1}|$, 现仅需考虑 $q_n\geqslant q>q_{n-1}$, 因 $p_nq_{n-1}-p_{n-1}q_n=(-1)^n$, 故方程组

$$\begin{cases} up_n+vp_{n-1}=p, \\ uq_n+vq_{n-1}=q \end{cases}$$

有解

$$\begin{aligned} u&=\pm(pq_{n-1}-qp_{n-1}), \\ v&=\pm(qp_n-pq_n). \end{aligned}$$

由于 $0<q_{n-1}<q\leqslant q_n$, u 和 v 不能都为正数. 若 $v=0$, 则 $p_n/q_n=p/q$, 与假设矛盾, 所以 u 与 v 一定是一正一负. 由定理 5.4 知

$$p_n-\alpha q_n, \quad p_{n-1}-\alpha q_{n-1}$$

也是一正一负, 故

$$u(p_n-\alpha q_n), \quad v(p_{n-1}-\alpha q_{n-1})$$

同号, 由

$$\begin{aligned} p-\alpha q&=up_n+vp_{n-1}-\alpha(uq_n+vq_{n-1}) \\ &=u(p_n-\alpha q_n)+v(p_{n-1}-\alpha q_{n-1}) \end{aligned}$$

可知

$$|p-\alpha q|>|p_{n-1}-\alpha q_{n-1}|>|p_n-\alpha q_n|,$$

证毕.

5.4　Legendre 判别条件

定理 5.8　α 的两个连续的连分数中至少有一个适合

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}.$$

证明　由定理 5.4 知, $\dfrac{p_n}{q_n}$ 与 $\dfrac{p_{n+1}}{q_{n+1}}$ 中有一个比 α 大, 有一个比 α 小, 故

$$\left|\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}\right|=\left|\frac{p_n}{q_n}-\alpha\right|+\left|\frac{p_{n+1}}{q_{n+1}}-\alpha\right|.$$

若定理不成立, 则有

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \geqslant \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2},$$

即 $(q_{n+1} - q_n)^2 \leqslant 0$, 这是不可能的, 定理得证.

当 α 为无理数时, 可知有无穷个分数 p/q, 使

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

考虑相反的一个问题, 则有如下定理.

定理 5.9 若有一有理数 p/q 适合

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2},$$

则 p/q 必为 α 的渐近分数.

证明 令

$$\alpha - \frac{p}{q} = \frac{\epsilon\delta}{q^2}, \quad \epsilon = \pm 1, \quad 0 < \delta < \frac{1}{2}. \tag{5.3}$$

将 p/q 展开为有限连分数

$$\frac{p}{q} = [a_0, a_1, \cdots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}},$$

但这种连分数展开并不是唯一的, 当 $a_{n-1} > 1$ 时,

$$[a_0, a_1, \cdots, a_{n-1}] = [a_0, a_1, \cdots, a_{n-1} - 1, 1];$$

当 $a_{n-1} = 1$ 时,

$$[a_0, a_1, \cdots, a_{n-1}] = [a_0, a_1, \cdots, a_{n-2} + 1],$$

所以总可以选择 n, 使 $\epsilon = (-1)^{n-1}$. 式 (5.3) 成为

$$\alpha - \frac{p_{n-1}}{q_{n-1}} = \frac{\epsilon\delta}{q_{n-1}^2}.$$

由下式定义 β:

$$\alpha = \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}, \tag{5.4}$$

因而

$$\begin{aligned}
\frac{(-1)^{n-1}\delta}{q_{n-1}^2} = \frac{\epsilon\delta}{q_{n-1}^2} &= \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} \\
&= \frac{-(p_{n-1}q_{n-2} - p_{n-2}q_{n-1})}{q_{n-1}(q_{n-1}\beta + q_{n-2})} \\
&= \frac{(-1)^{n-1}}{q_{n-1}(q_{n-1}\beta + q_{n-2})},
\end{aligned}$$

由此推得

$$\frac{1}{q_{n-1}\beta+q_{n-2}}<\frac{1}{2q_{n-1}}.$$

因此

$$q_{n-1}\beta>2q_{n-1}-q_{n-2}>q_{n-1},$$

所以 $\beta>1$, 由式 (5.4) 可知

$$\alpha=[a_0,a_1,\cdots,a_{n-1},\beta],$$

可见

$$\frac{p}{q}=\frac{p_{n-1}}{q_{n-1}}=[a_0,a_1,\cdots,a_{n-1}]$$

是 α 的渐近分数, 证毕.

习 题

习题 5.1 序列$\{u_n\}$: $1,1,2,3,5,8,13,21,\cdots(u_1=u_2=1,u_{i+1}=u_i+u_{i-1}\ (i>1))$ 称为 Fibonacci 序列. 试证 $\alpha=\frac{1}{2}(1+\sqrt{5})$ 的第 n 个渐近分数为 $\frac{u_{n+2}}{u_{n+1}}$.

习题 5.2 (1) 已知圆周率 $\pi=[3,7,15,1,292,1,1,\cdots]$, 试求 π 的前 6 个渐近分数. 由此可见, 祖冲之得到的疏率 $\frac{22}{7}$ 及密率 $\frac{355}{113}$ 都是渐近分数.

(2) 在分母不超过113的分数中, 没有数比 $\frac{355}{113}$ 更接近 π.

习题 5.3 设

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}=\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix},\quad n>1,$$

证明

$$\frac{p_n}{q_n}=[a_0,a_1,\cdots,a_n].$$

习题 5.4 证明若 $a_0=0,a_1=1$, 且对 $n\geqslant 2$, $a_n=2a_{n-1}+a_{n-2}$, 那么

$$a_n=\frac{(1+\sqrt{2})^n-(1-\sqrt{2})^n}{2\sqrt{2}}.$$

第 6 章　代 数 数 域

代数数域是代数数论的研究对象, 代数数论的起源可追溯到 Gauss 研究二平方和问题时涉及的 Gauss 整环 $\mathbb{Z}[\mathrm{i}]$ 和 Kummer 研究 Fermat 大定理时涉及的分圆环 $\mathbb{Z}[\zeta_p]$, 它的大部分经典理论产生于 19 世纪. 20 世纪 70 年代以来, 许多公钥密码体制的产生和各种相应攻击方法的出现, 不仅利用了代数数论的理论, 而且促进了计算代数数论学科的发展. 目前, 有限域上离散对数问题和大整数分解问题求解的最好算法是数域筛法, 它涉及代数数论的许多结果. 本章的目的仅仅是介绍一些代数数论的基本理论, 便于理解 10.5 节中的数域筛法.

6.1　代 数 整 数

有理数域 $\mathbb{Q}$ 的一个有限扩张 K, 称作代数数域. 由本原元素定理可知, K 一定是单扩张, 即 $K=\mathbb{Q}(\theta)$. 设 $f(x)$ 是 θ 的极小多项式, 且 $\deg f(x)=n$, 显然 $K=\mathbb{Q}(\theta)=\mathbb{Q}[x]/(f(x))$. 故将 K 看成 $\mathbb{Q}$ 上的 n 维线性空间, $\{1, \theta, \cdots, \theta^{n-1}\}$ 是其一组基.

$f(x)$ 在复数域 $\mathbb{C}$ 上可以完全分解

$$f(x)=\prod_{j=1}^{n}(x-\theta_i).$$

由于复根成对出现, 可设 $f(x)$ 有 r_1 个实根, r_2 对复根, 那么 $n=r_1+2r_2$. 现对 $\{\theta_i\}_{1\leqslant i\leqslant n}$ 重新排序, 不妨设

$$\begin{aligned}&\theta_1,\cdots,\theta_{r_1}\in\mathbb{R},\\&\theta_{r_1+1},\cdots,\theta_n\in\mathbb{C}\setminus\mathbb{R},\end{aligned}$$

且

$$\theta_{r_1+r_2+j}=\overline{\theta}_{r_1+j}\quad(1\leqslant j\leqslant r_2),\quad n=r_1+2r_2.$$

令 σ_i 是 $K\longrightarrow K_i=\mathbb{Q}(\theta_i)$ 的同构映射, $1\leqslant i\leqslant n$, 对 K 中任意 n 个元素 $\alpha_1,\cdots,\alpha_n$, 称

$$d_K(\alpha_1,\cdots,\alpha_n)=\det(\sigma_i(\alpha_j))^2_{1\leqslant i,j\leqslant n}$$

为元素 $\{\alpha_1,\cdots,\alpha_n\}$ 的判别式. 特别地, $\{1,\theta,\cdots,\theta^{n-1}\}$ 的判别式也称作 $f(x)$ 的判别式, 记作 $\Delta(f)$.

设 $f(x)=x^d+c_{d-1}x^{d-1}+\cdots+c_0$, 那么 $f'(x)=dx^{d-1}+\cdots+c_1$, 定义 $\mathrm{res}\,(f,f')$ 为矩阵

$$M=\begin{pmatrix}1 & c_{d-1} & \cdots & \cdots & c_1 & c_0 & & \\ & 1 & c_{d-1} & \cdots & & & & \\ & & \ddots & & & & & \\ & & & 1 & c_{d-1} & \cdots & \cdots & c_0\\ d & (d-1)c_{d-1} & \cdots & & c_1 & \cdots & \cdots & \\ & d & \cdots & & \cdots & \cdots & \cdots & \\ & & \ddots & & & & & \\ & & & & d & (d-1)c_{d-1} & \cdots & c_1\end{pmatrix}$$

的行列式, 称作 f 和 f' 的结式, 可证 (见习题 6.1):

$$\Delta(f)=\prod_{1\leqslant i<j\leqslant n}(\theta_i-\theta_j)^2=(-1)^{\frac{n(n-1)}{2}}N(f'(\theta))=(-1)^{\frac{n(n-1)}{2}}\mathrm{res}\,(f,f').$$

取 L 是 $K/\mathbb{Q}$ 的中间域, $\mathbb{Q}\subseteq L\subseteq K$, K 看成 L-线性空间, 对任意 $\alpha\in K$, 定义 L-线性变换

$$L_\alpha: K\longrightarrow K$$
$$\beta\longmapsto\alpha\cdot\beta,$$

称此线性变换的范和迹为 α 的范和迹, 分别记作 $N_{K/L}(\alpha)$ 和 $T_{K/L}(\alpha)$. 在取 $L=\mathbb{Q}$ 时, 常用 N,T 分别记作 $N_{K/\mathbb{Q}},T_{K/\mathbb{Q}}$. 可以证明 $N_{K/L}$ 和 $T_{K/L}$ 满足下面性质 (见习题 6.2).

(1) 对任意 $\alpha,\beta\in K$,

$$N_{K/L}(\alpha\beta)=N_{K/L}(\alpha)N_{K/L}(\beta),\quad T_{K/L}(\alpha+\beta)=T_{K/L}(\alpha)+T_{K/L}(\beta);$$

(2) 对于 $\alpha\in L$, $N_{K/L}(\alpha)=\alpha^d$, $T_{K/L}(\alpha)=d\cdot\alpha$, 其中 $d=[K:L]$;

(3) 设 $\mathbb{Q}\subseteq M\subseteq L\subseteq K$ 是数域链, 对于 $\alpha\in K$,

$$N_{K/M}(\alpha)=N_{L/M}\left(N_{K/L}(\alpha)\right),\quad T_{K/M}(\alpha)=T_{L/M}\left(T_{K/L}(\alpha)\right);$$

(4) $N(\alpha)=\prod\limits_{i=1}^{n}\sigma_i(\alpha)$, $T(\alpha)=\sum\limits_{i=1}^{n}\sigma_i(\alpha)$.

引理 6.1　令 $\alpha\in K$, 设 α 的极小多项式为

$$f(x)=x^d-a_1x^{d-1}+\cdots+(-1)^da_d\in\mathbb{Q}[x],$$

则 $N(\alpha)=a_d^{\frac{n}{d}}$, $T(\alpha)=\dfrac{n}{d}a_1$.

证明 令 $L=\mathbb{Q}(\alpha)$, 那么

$$N_{K/\mathbb{Q}}(\alpha)=N_{L/\mathbb{Q}}(N_{K/L}(\alpha))=N_{L/\mathbb{Q}}(\alpha^{\frac{n}{d}})=N_{L/\mathbb{Q}}(\alpha)^{\frac{n}{d}},$$
$$T_{K/\mathbb{Q}}(\alpha)=T_{L/\mathbb{Q}}(T_{K/L}(\alpha))=T_{L/\mathbb{Q}}\left(\frac{n}{d}\alpha\right)=\frac{n}{d}T_{L/\mathbb{Q}}(\alpha).$$

因为 $\{1,\alpha,\cdots,\alpha^{d-1}\}$ 是 $L/\mathbb{Q}$ 的一组基,

$$\begin{aligned}\alpha\cdot\begin{pmatrix}1\\ \alpha\\ \vdots\\ \alpha^{d-1}\end{pmatrix}&=\begin{pmatrix}\alpha\\ \alpha^2\\ \vdots\\ \alpha^{d}\end{pmatrix}\\ &=\begin{pmatrix}0&1&0&\cdots&0&0\\ 0&0&1&\cdots&0&0\\ \vdots&\vdots&\vdots&&\vdots&\vdots\\ 0&0&0&\cdots&0&1\\ (-1)^{d-1}a_d&(-1)^{d-2}a_{d-1}&(-1)^{d-3}a_{d-2}&\cdots&-a_2&a_1\end{pmatrix}\begin{pmatrix}1\\ \alpha\\ \vdots\\ \alpha^{d-1}\end{pmatrix},\end{aligned}$$

所以

$$N_{L/\mathbb{Q}}(\alpha)=\det\begin{pmatrix}0&1&0&\cdots&0&0\\ 0&0&1&\cdots&0&0\\ \vdots&\vdots&\vdots&&\vdots&\vdots\\ 0&0&0&\cdots&0&1\\ (-1)^{d-1}a_d&(-1)^{d-2}a_{d-1}&(-1)^{d-3}a_{d-2}&\cdots&-a_2&a_1\end{pmatrix}=a_d,$$

$T_{L/\mathbb{Q}}(\alpha)=a_1$, 证毕.

容易看出 $d_K(\alpha_1,\cdots,\alpha_n)=\det(\mathrm{tr}(\alpha_i\alpha_j))$ 是一个 $\mathbb{Q}$ 上的 n 阶方阵的行列式, 且可证 $\{\alpha_1,\cdots,\alpha_n\}$ 是一组 $\mathbb{Q}$-基当且仅当 $d_K(\alpha_1,\cdots,\alpha_n)\neq 0$(见习题 6.3).

首一整系数多项式的根称作代数整数, 易证一个代数数是代数整数当且仅当其极小多项式是整系数多项式, 不失一般性, 可以要求 K 的生成元 θ 为代数整数 (见习题 6.4). 以后均在此条件下讨论. 显然代数整数的范和迹是整数, 特别地, 一组代数整数 $\alpha_1,\cdots,\alpha_n$ 的判别式 $d_K(\alpha_1,\cdots,\alpha_n)\in\mathbb{Z}$. 下面给出代数整数的其他一些刻画.

定理 6.1 对 $\alpha\in\mathbb{C}$(复数域), 下面几个条件相互等价:

(1) α 是代数整数;

(2) 环 $\mathbb{Z}[\alpha]$ 是有限生成 $\mathbb{Z}$-模;

(3) α 是 $\mathbb{C}$ 中某个非零子环 R 中的元素, 并且 R 看成 $\mathbb{Z}$-模是有限生成的;

(4) 存在有限生成 $\mathbb{Z}$-模 $A\subseteq\mathbb{C}$, 使得 $\alpha A\subseteq A$.

证明 (1)$\Longrightarrow$(2) 因为 α 是代数整数, 由定义可知, 任意 $\alpha^m(m \geqslant 0)$ 都能写成 $1, \alpha, \cdots, \alpha^{d-1}$ 的整系数的线性组合, 其中 $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, 故 $\mathbb{Z}[\alpha]$ 是有限生成 $\mathbb{Z}$-模.

(2)$\Longrightarrow$(3) 取 $R = \mathbb{Z}[\alpha]$.

(3)$\Longrightarrow$(4) 取 $A = R$.

(4)$\Longrightarrow$(1) 设 $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, 因为 $\alpha A \subseteq A$, 所以存在整系数矩阵 M, 使得

$$\begin{pmatrix} \alpha\alpha_1 \\ \vdots \\ \alpha\alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix},$$

即

$$(\alpha I_n - M) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0.$$

于是 α 便为首一整系数多项式 $\det(xI_n - M) = 0$ 的根, 证毕.

由定理 6.1 可推出所有代数整数构成一个环 (见习题 6.5), 将 K 中所有代数整数构成的子环记作 O_K, 容易证明 $O_K \cap \mathbb{Q} = \mathbb{Z}$(见习题 6.6), 即 $\alpha \in \mathbb{Q}$ 是代数整数当且仅当 $\alpha \in \mathbb{Z}$.

引理 6.2 设 $K = \mathbb{Q}(\theta)$, θ 的极小多项式 $f(x) \in \mathbb{Z}[x]$, 令

$$\frac{f(x)}{x-\theta} = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1}, \quad \beta_i \in K,$$

那么, $\dfrac{\beta_0}{f'(\theta)}, \cdots, \dfrac{\beta_{n-1}}{f'(\theta)}$ 是 K 的一组 $\mathbb{Q}$-基, 且

$$T\left(\theta^i \frac{\beta_j}{f'(\theta)}\right) = \delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

证明 设 f 的所有不同的根为 $\theta_1, \cdots, \theta_n$, 那么对任意 $0 \leqslant r \leqslant n-1$,

$$g(x) = \sum_{i=1}^{n} \frac{f(x)}{(x-\theta_i)} \frac{\theta_i^r}{f'(\theta_i)} - x^r$$

是 $n-1$ 次多项式, 然而容易看出 $\theta_1, \cdots, \theta_n$ 仍是 $g(x)$ 的根, 故

$$\sum_{i=1}^{n} \frac{f(x)}{(x-\theta_i)} \frac{\theta_i^r}{f'(\theta_i)} = x^r.$$

比较两边 x^j 的系数

$$\sum_{i=1}^{n}\sigma_i(\beta_j)\frac{\sigma_i(\theta)^r}{\sigma_i(f'(\theta))}=\delta_{j,r},$$

即 $T\left(\theta^r\frac{\beta_j}{f'(\theta)}\right)=\delta_{j,r}$, 由此可知 $\frac{\beta_0}{f'(\theta)},\cdots,\frac{\beta_{n-1}}{f'(\theta)}$ 是一组基, 证毕.

引理 6.3 符号同引理6.2, 则

$$O_K\subseteq\mathbb{Z}\frac{\beta_0}{f'(\theta)}+\cdots+\mathbb{Z}\frac{\beta_{n-1}}{f'(\theta)}=\frac{\mathbb{Z}[\theta]}{f'(\theta)}.$$

证明 任取 $\alpha\in O_K$, 相对于基 $\frac{\beta_0}{f'(\theta)},\cdots,\frac{\beta_{n-1}}{f'(\theta)}$, α 能写成

$$\alpha=a_0\frac{\beta_0}{f'(\theta)}+\cdots+a_{n-1}\frac{\beta_{n-1}}{f'(\theta)},\quad a_i\in\mathbb{Q}.$$

由引理 6.2 可知 $a_i=T(\alpha\theta^i)$, $0\leqslant i\leqslant n-1$, 故由引理 6.1 知 $a_i\in\mathbb{Z}$. 比较等式 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0=(x-\theta)(\beta_0+\beta_1x+\cdots+\beta_{n-1}x^{n-1})$ 两边 $x^i(1\leqslant i\leqslant n)$ 的系数, 得

$$\begin{aligned}
&\beta_{n-1}=1,\\
&\beta_{n-2}=\theta+a_{n-1},\\
&\beta_{n-3}=\theta^2+a_{n-1}\theta+a_{n-2},\\
&\qquad\cdots\cdots\\
&\beta_0=\theta^{n-1}+a_{n-1}\theta^{n-2}+\cdots+a_2\theta+a_1,
\end{aligned}$$

故 $\mathbb{Z}\beta_0+\cdots+\mathbb{Z}\beta_{n-1}=\mathbb{Z}[\theta]$, 证毕.

定义 6.1 K 的一个阶(order)是 K 中的一个子环, 且看成 $\mathbb{Z}$-模是维数为 $n=[K:\mathbb{Q}]$ 的自由模.

引入一个 $\mathbb{Q}$-向量空间 K 上的双线性映射

$$\begin{aligned}
\langle\ ,\ \rangle:K\times K&\longrightarrow R\\
(x,y)&\longmapsto\sum_{i=1}^{n}\sigma_i(x)\overline{\sigma_i(y)},
\end{aligned}$$

上式右边常记作 $\langle x,y\rangle$. 由此诱导出 K 上的长度函数

$$\begin{aligned}
L:K&\longrightarrow R\geqslant 0\\
x&\longmapsto\langle x,x\rangle.
\end{aligned}$$

取定 K 的一组基 $\alpha_1,\cdots,\alpha_n$, 设 $x=\sum\limits_{i=1}^{n}x_i\alpha_i$, L 变成了一个正定二次型

$$L(x)=(x_1,\cdots,x_n)A\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix},$$

其中 $A=(\langle\alpha_i,\alpha_j\rangle)_{1\leqslant i,j\leqslant n}$. 特别地, 将系数 $x_1,\cdots,x_n$ 限制在 $\mathbb{Z}$ 中,n 维自由 $\mathbb{Z}$-模 $M=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$ 和 L 一起看成一般意义下的格, 此格的判别式为 $d(M)=\det(A)^{\frac{1}{2}}$, 注意到, 若 $\alpha_1,\cdots,\alpha_n$ 均是代数整数, 那么 $d(M)^2=\det(A)=|d_K(\alpha_1,\cdots,\alpha_n)|\in\mathbb{Z}$(见习题 6.7).

引理 6.4　O_K 是 K 中的最大阶.

证明　取 K 中一个阶 A, $\forall\alpha\in A$, 因为 $\alpha A\subseteq A$, 由定理 6.1(4) 可知 $\alpha\in O_K$, 即 $A\subseteq O_K$. 现证 O_K 是维数为 n 的自由 $\mathbb{Z}$-模. 设

$$S=\Big\{M\subseteq O_K|\ M\text{是维数为 } n \text{ 的 } \mathbb{Z}\text{-模}\Big\},$$

因为 $\mathbb{Z}[\theta]\in S$, 故 $S\neq\varnothing$. 又因为 $d(M)^2$ 是正整数, 所以一定存在 $\wedge=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n\in S$ 使得

$$d(\wedge)=\min\{d(M)|\ M\in S\}.$$

断言 $\wedge=O_K$, 否则存在 $\alpha\in O_K\backslash\wedge$, 令

$$\alpha=\sum_{i=1}^{n}a_i\alpha_i,\quad a_i\in\mathbb{Q},$$

必存在 $a_i\notin\mathbb{Z}$, 不妨设 $a_1\notin\mathbb{Z}$, 即 $a_1=[a_1]+r$, $0<r<1$, $r\in\mathbb{Q}$. 令 $\overline{\alpha}=\alpha-[a_1]\alpha_1\in O_K$, $\overline{\alpha}_1=\overline{\alpha}$, $\overline{\alpha}_i=\alpha_i$, $2\leqslant i\leqslant n$. 显然 $\overline{\wedge}=\mathbb{Z}\overline{\alpha}_1+\cdots+\mathbb{Z}\overline{\alpha}_n\in S$, 而 $d(\overline{\wedge})=rd(\wedge)<d(\wedge)$, 这和 $\wedge$ 的选择矛盾, 证毕.

以后称 O_K 的一组 $\mathbb{Z}$-基为 K 的整基. 注意到对 K 的一个阶 O 的任两组基 $\{\alpha_1,\ \cdots,\ \alpha_n\}$, $\{\beta_1,\ \cdots,\ \beta_n\}$, 一定存在整系数的可逆矩阵 M(等价 $\det M=\pm1$) 使得

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=M\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix},$$

故 $d_K(\alpha_1,\cdots,\alpha_n)=(\det M)^2d_K(\beta_1,\cdots,\beta_n)=d_K(\beta_1,\cdots,\beta_n)$, 即此整数对基的选择无关, 称此整数为 O 的判别式, 记作 $d_K(O)$. 特别地, K 的任一组整基的判别式称作 K 的判别式, 记作 Δ_K.

6.2 Dedekind 整 环

令 R 是一个含幺交换环.

定义 6.2 R 称作 Noether 环, 如果 R 的每个理想都是有限生成的.

Noether 环的等价条件(见习题 6.10) 下列条件是等价的:

(1) R 是 Noether 环;

(2) R 的理想升链一定有限, 即

$$A_1 \subseteq \cdots \subseteq A_n \subseteq \cdots$$

是 R 的理想链, 那么一定存在 $k \in \mathbb{N}$ 使得 $A_k = A_{k+1} = \cdots$;

(3) R 的任意一个由理想构成的非空集合一定有极大元.

定义 6.3 整环 R 称作整闭的, 如果 R 的分式域 K 中任一个以 $R[x]$ 中某一个首一多项式为根的元素一定在 R 中.

定义 6.4 整环 R 称作 Dedekind 整环, 如果 R 满足如下三个条件:

(1) R 是 Noether 环;

(2) R 中每个非零素理想一定是极大理想;

(3) R 是整闭的.

定理 6.2 设 A 是 K 的一个阶, 那么, A 是Noether的, 且任一非零素理想一定是极大理想. 特别地, O_K 是Dedekind整环.

证明 任一 $I \neq 0$ 是 A 的理想, 因为 A 是 n 维自由 $\mathbb{Z}$-模, 故 I 看成 $\mathbb{Z}$-子模, 也是自由模, 且维数 $\leqslant n$. 然而对 A 的任何一组基 $\alpha_1, \cdots, \alpha_n$, 取 $0 \neq r \in I$, 那么 $r\alpha_1, \cdots, r\alpha_n$ 是 I 的一个 $\mathbb{Z}$-线性无关组, 故 I 也是一个 n 维自由 $\mathbb{Z}$-模, 将其看成 A-模显然是有限生成的, 即 A 是 Noether 环. 再由 Abel 基本定理可知, A/I 是有限群, 特别地, 取 $I = \mathfrak{p}$ 是素理想时, $A/\mathfrak{p}$ 是有限整环, 因此是域, 故 $\mathfrak{p}$ 是极大理想. 现只需证 O_K 是整闭的, 任取 $\alpha \in K$ 满足: $\alpha^d + c_1\alpha^{d-1} + \cdots + c_d = 0$, 其中 $c_i \in O_K, 1 \leqslant i \leqslant d$. 令 $R = \mathbb{Z}[c_1, \cdots, c_d]$ 是由 $c_1, \cdots, c_d$ 生成的 O_K 的子环, 显然作为 $\mathbb{Z}$-模是有限生成的, 且 $R[\alpha] = R + R\alpha + \cdots + R\alpha^{d-1}$ 作为 $\mathbb{Z}$-模也是有限生成的, 由定理 6.1(3) 知 $\alpha \in O_K$, 证毕.

上述证明过程表明, A 的任意一个非零理想 I 都是 n 维自由 $\mathbb{Z}$-模, A 的任一组 $\mathbb{Z}$-基的判别式定义为 A 的判别式, 记作 $d(A)$.

设 $\mathfrak{a}$ 是 A 的一个理想, 商环 $A/\mathfrak{a}$ 是有限环, 称 $|A/\mathfrak{a}|$ 为 $\mathfrak{a}$ 的范, 记作 $N(\mathfrak{a})$, 当 $\mathfrak{a} = \mathfrak{p}$ 是 A 的一个非零素理想, $A/\mathfrak{p}$ 是有限域, 存在唯一的素数 p 和正整数 e, 使得

$$A/\mathfrak{p} = F_{p^e},$$

$e=[A/\mathfrak{p}:F_p]$ 称作 $\mathfrak{p}$ 的次数, 记作 $\deg(\mathfrak{p})$, $|A/\mathfrak{p}|=p^{\deg\mathfrak{p}}$.

理想的范映射 N 满足 (见习题 6.11)

(1) $|N(x)|=N(xA)$, 特别地, $A=O_K$ 时, N 还满足

(2) $N(\mathfrak{a}\cdot\mathfrak{b})=N(\mathfrak{a})N(\mathfrak{b})$,

(3) $d_K(\mathfrak{a})=N(\mathfrak{a})^2\Delta_K$.

定理 6.3 Dedekind整环中任一个非平凡理想能唯一(不计顺序)表示成一些素理想的乘积.

证明 参见文献 [53].

令 $I^\circ(O_K)$ 为 O_K 中的全体非零理想构成的集合, $I^\circ(O_K)$ 中的每一个元素 I 均能唯一写成素理想的乘积, 即

$$I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}.$$

显然 $I^\circ(O_K)$ 对于理想的乘积构成一个交换的含幺半群, 且满足消去律.

设素数 p, 在 O_K 中提升获得的理想

$$pO_K=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$$

若存在 $e_i\neq 1(1\leqslant i\leqslant g)$, 称 p 在 K 中分歧, 否则称 p 在 K 中不分歧.

定理 6.4 设 p 为素数, K 为代数数域, 则 p 在 K 中分歧当且仅当 $p\,|\,\Delta_K$.

证明 参见文献 [53].

对 O_K 的任一素理想 $\mathfrak{p}$, 定义映射 $\nu_{\mathfrak{p}}:I^\circ(O_K)\longrightarrow N\cup\{0\}$. $\nu_{\mathfrak{p}}(I)$ 表示在 I 的分解式中 $\mathfrak{p}$ 因子出现的个数, 显然 $\nu_{\mathfrak{p}}$ 是半群同态, 且 I 可写成

$$I=\prod_{\mathfrak{p}}\mathfrak{p}^{\nu_{\mathfrak{p}}(I)}.$$

由于含幺半群 $I^\circ(O_K)$ 满足消去律, 可将 $I^\circ(O_K)$ 扩充成一个群. 具体地, 在 $I^\circ(O_K)\times I^\circ(O_K)$ 中定义一个关系 $\sim$, 若 $(A,B)\sim(C,D)$ 当且仅当 $BC=AD$, 可证 $\sim$ 是等价关系, 且

$$I^\circ(O_K)\times I^\circ(O_K)/\sim$$

是一个群. (A,B) 所在的等价类记作 $\dfrac{A}{B}$, 取 B 中的一个非零元 α, 由于 $(\alpha)\subseteq B$, 那么一定存在理想 $C\in I^\circ(O_K)$ 使

$$BC=(\alpha).$$

这样, $\alpha\cdot\dfrac{A}{B}\in I^\circ(O_K)$. 下面将 $\dfrac{A}{B}$ 赋予实际含义.

定义 6.5 K 的一个子集合 F, 若满足存在 $\alpha \in O_K$ 使得 αF 是 O_K 的理想, 称 F 是 K 的分式理想. 全体分式理想构成的集合为 $I(O_K)$. 以后 O_K 中的理想也称整理想, 任意 $x \in K^*$, xO_K 称作主分式理想.

容易证明

$$I(O_K) \cong I^\circ(O_K) \times I^\circ(O_K)/\sim .$$

这样 $\nu_\mathfrak{p}$ 自然可以提升到从 $I(O_K)$ 到 $\mathbb{Z}$ 的一个群同态, (O_K) 中任一个分式理想 F, 有如下唯一表示

$$F = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(F)}.$$

将从 K^* 到 $I(O_K)(: x \mapsto xO_K)$ 群同态和 $\nu_\mathfrak{p}$ 结合, 仍记作 $\nu_\mathfrak{p}$, 便可视 $\nu_\mathfrak{p}$ 为 $K^* \longrightarrow \mathbb{Z}$ 的一个群同态, 且满足性质: 对于任意 $x \in K^*$, 几乎对所有 $\nu_\mathfrak{p}$(除有限个外), 均有 $\nu_\mathfrak{p}(x) = 0$, 且 $|N(x)| = \prod_\mathfrak{p} N(\mathfrak{p})^{\nu_\mathfrak{p}(x)}$. 同态 $\nu_\mathfrak{p}$ 也称作 K 的 p-adic 赋值.

定义 6.6 令 $P(O_K)$ 为主分式理想构成的一个集合, 称商群 $I(O_K)/P(O_K)$ 为 K 的类群, 记作 $Cl(O_K)$.

对于 K 的一个理想 $\mathfrak{a}$ 一定是 n 维自由 $\mathbb{Z}$-模, 函数 L 实际上给出了 $\mathfrak{a}$ 中元素的一种 "长度", 事实上 $(\mathfrak{a}, L)$ 是一般意义下的格. 我们用如下映射可将它看成 $\mathbb{R}^n$ 在 $\|\cdot\|$ 意义的格 (参见 13.2 节), 定义

$$\begin{aligned} \sigma : K &\longrightarrow \mathbb{R}^n \\ \alpha &\longmapsto \Big(\alpha^{(1)}, \cdots, \alpha^{(r_1)}, \sqrt{2}\mathrm{Re}(\alpha^{(r_1+1)}), \cdots, \sqrt{2}\mathrm{Re}(\alpha^{(r_1+r_2)}), \\ &\quad \sqrt{2}\mathrm{Im}(\alpha^{(r_1+1)}), \cdots, \sqrt{2}\mathrm{Im}(\alpha^{(r_1+r_2)})\Big). \end{aligned} \tag{6.1}$$

$\mathrm{Re}(\cdot)$ 表示 $\cdot$ 的实部, $\mathrm{Im}(\cdot)$ 表示 $\cdot$ 的虚部, $\alpha^{(i)}$ 记作 $\sigma_i(\alpha)$, 可直接验证 σ 是群的单同态, 进而 $(\sigma(\mathfrak{a}), \|\cdot\|)$ 是 $\mathbb{R}^n$ 中的一个格, 且满足

(1) $L(\alpha) = \|\sigma(\alpha)\|^2$;

(2) $d(\mathfrak{a}) = d(\sigma(\mathfrak{a}))^2$, 即理想 $\mathfrak{a}$ 的判别式等于格 $\sigma(\mathfrak{a})$ 的判别式的平方 (见习题 6.12).

引理 6.5 类群 $Cl(O_K)$ 中的任一个理想类, 均包含一个整理想 $\mathfrak{a}$, 使得

$$N(\mathfrak{a}) \leqslant \frac{1}{n^{\frac{n}{2}}} 2^{\frac{n(n-1)}{4}} \sqrt{|\Delta_K|} \ .$$

证明 对任意 $\overline{F} \in Cl(O_K), F \in I(O_K)$, 取一个整理想 $\mathfrak{a} \in \overline{F^{-1}}$. 设 $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, 那么格 $\sigma(\mathfrak{a}) = \mathbb{Z}\sigma\alpha_1 + \cdots + \mathbb{Z}\sigma\alpha_n$. 取 $x_1, \cdots, x_n$ 是格 $\sigma(\mathfrak{a})$ 的一组 L^3-约化基, 由定理 13.6 知

$$\|x_1\|^2 \leqslant 2^{\frac{(n-1)}{2}} d(\sigma(\mathfrak{a}))^{\frac{2}{n}} .$$

又因为存在 $\beta_1 \in \mathfrak{a}$, 使得 $x_1 = \sigma(\beta_1)$, 再由算术平均值大于等于几何平均值, 可得

$$\begin{aligned}\left\|x_1\right\|^2 = \left\|\sigma(\beta_1)\right\|^2 = L(\beta_1) &= \sum_{i=1}^{n} \sigma_i(\beta_1) \cdot \overline{\sigma_i(\beta_1)} \\ &= \sum_{i=1}^{n} \left\|\beta_1^{(i)}\right\|^2 \geqslant n \cdot \left(\prod_{i=1}^{n} \left\|\beta_1^{(i)}\right\|^2\right)^{\frac{1}{n}} = n|N(\beta_1)|^{\frac{2}{n}},\end{aligned}$$

所以

$$|N(\beta_1)| \leqslant \left(\frac{\|x_1\|^2}{n}\right)^{\frac{n}{2}} \leqslant \frac{1}{n^{\frac{n}{2}}} 2^{\frac{n(n-1)}{4}} d\left(\sigma(\mathfrak{a})\right).$$

而 $d\left(\sigma(\mathfrak{a})\right) = \sqrt{d(\mathfrak{a})} = N(\mathfrak{a})\sqrt{|\Delta_K|}$, 故 $|N(\beta_1)| \leqslant n^{-\frac{n}{2}} \cdot 2^{\frac{n(n-1)}{4}} N(\mathfrak{a})\sqrt{|\Delta_K|}$.

因为 $\beta_1 \in \mathfrak{a}$, 即 $(\beta_1) \subseteq \mathfrak{a}$, 所以存在整理想 $\mathfrak{b}$, 使得 $\mathfrak{a} \cdot \mathfrak{b} = (\beta_1)$, 那么 $N(\mathfrak{a}) \cdot N(\mathfrak{b}) = N\left((\beta_1)\right) = |N(\beta_1)|$, 于是

$$N(\mathfrak{b}) = \frac{|N(\beta_1)|}{N(\mathfrak{a})} \leqslant n^{-\frac{n}{2}} 2^{\frac{n(n-1)}{4}} \sqrt{|\Delta_K|},$$

证毕.

事实上, 上述引理的上界 $n^{-\frac{n}{2}} 2^{\frac{n(n-1)}{4}} \sqrt{|\Delta_K|}$ 还能进一步改进, 最著名的一个界称作 Minkowski 界

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|},$$

它可由定理 13.4 推得, 参见文献 [53].

定理 6.5　*类群 $Cl(O_K)$ 是有限群.*

证明　由引理 6.5, 只需证明对给定正整数 m, 满足 $N(\mathfrak{a}) = m$ 的整理想只有有限多个. 因为 $m = N(\mathfrak{a}) = |O_K/\mathfrak{a}|$, 所以 $m \in \mathfrak{a}$, 即 $\mathfrak{a}$ 是 (m) 的因子, 故 $\mathfrak{a}$ 只有有限多个, 证毕.

具体求类数 h_K 是一个十分困难的问题, 不再证明地给出上界.

定理 6.6

$$h_K \leqslant M_K \frac{(n - 1 + \log M_K)^{n-1}}{(n-1)!}.$$

证明　参见文献 [29].

显然 $h_K = 1$ 当且仅当 O_K 是主理想整环, 这等价于 O_K 是唯一分解整环 (见习题 6.13). 因而 h_K 的大小从某一侧面反映了 O_K 离主理想整环的远近.

设 U_K 为 O_K 中的所有可逆元构成的乘法群, 由 Abel 基本定理知

$$U_K = W_K \times F_K,$$

W_K 是 U_K 的扭子群, 即 U_K 中的所有有限阶元 (此时即为单位根) 全体, F_K 为 U_K 的自由部分.

引理 6.6(见习题 6.14) $\alpha \in O_K$, 那么

(1) $\alpha \in U_K$ 当且仅当 $|N(\alpha)| = 1$;

(2) $\alpha \in W_K$ 当且仅当对任意 $1 \leqslant i \leqslant n$, $|\sigma_i(\alpha)| = 1$.

构造对数嵌入映射

$$\begin{aligned} \ell : U_K &\longrightarrow \mathbb{R}^{r_1+r_2} \\ \alpha &\longmapsto \left(\lambda_i \log |\alpha^{(i)}|\right)_{1 \leqslant i \leqslant r_1+r_2}, \end{aligned}$$

其中

$$\lambda_i = \begin{cases} 1, & 1 \leqslant i \leqslant r_1, \\ 2, & r_1 + 1 \leqslant i \leqslant r_1 + r_2. \end{cases}$$

由引理 6.6 容易看出 ℓ 是群同态, $\ker \ell = W_K$, 且

$$\ell(U_K) \subseteq \left\{(x_1, \cdots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \,|\, x_1 + \cdots + x_{r_1+r_2} = 0\right\} \overset{\triangle}{=} H.$$

H 是超平面, 其维数为 $r_1 + r_2 - 1$, 而 $F_K \cong U_K/W_K = U_K/\ker \ell \cong \ell(U_K) \subseteq H$.

$\mathbb{R}^n$ 的一个加法子群 D 称作离散的, 是指对 $\mathbb{R}^n$ 中每个有界子集 B, 均有 $|D \cap B| < +\infty$. $\mathbb{R}^n$ 中的任一离散子群一定是 $\mathbb{R}^n$ 中某个 r $(0 \leqslant r \leqslant n)$ 维子空间中的格 (见习题 6.15).

定理 6.7 $\ell(U_K)$ 是一自由 $\mathbb{Z}$-模, 且维数 $\leqslant r_1 + r_2 - 1$.

证明 断言 $\ell(U_K)$ 是离散子群, 对 $\mathbb{R}^{r_1+r_2}$ 中的任一有界区域 B 取 $x \in \ell(U_K) \cap B$, $x = \ell(\alpha)$, $\alpha \in U_K$.

因为存在常数 M, 使得$|\alpha^{(i)}| \leqslant M$ $(1 \leqslant i \leqslant r_1)$, $|\alpha^{(i)}|^2 \leqslant M$ $(r_1+1 \leqslant i \leqslant r_1+r_2)$, 于是 α 所在的零化多项式 $f(x) = \prod\limits_{i=1}^{n} (x - \alpha^{(i)})$ 的各个系数是有界的. 而这样的多项式只有有限多个, 故 α 只能取有限个值, 即 $|\ell(U_K) \cap B| < +\infty$.

由习题 6.14 知 $\ell(U_K)$ 是 H 的某个子空间中的一个格, 即 $\ell(U_K)$ 是一个自由 $\mathbb{Z}$-模, 且维数 $\leqslant r_1 + r_2 - 1$, 证毕.

下面要说明 $\ell(U_K)$ 中存在 $r_1 + r_2 - 1$ 个元素组成的 $\mathbb{Z}$-线性无关组. 易见, 对数嵌入 ℓ 可以扩展定义到 O_K 上.

引理 6.7 令 $\alpha \in O_K$, 设 $\ell(\alpha) = (a_1, \cdots, a_{r_1+r_2})$, 则对任意 $k \in \{1, \cdots, r_1+r_2\}$, 存在 $\beta \in O_K$ 满足

(1) $b_i < a_i$, 若 $i \neq k$;

(2) $|N(\beta)| \leqslant \left(\dfrac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$,

其中 $\ell(\beta) = (b_1, \cdots, b_{r_1+r_2})$.

证明　不妨设 $k = 1$, 记 σ 是式 (6.1) 的映射, 取常数 c_i $(2 \leqslant i \leqslant r_1 + r_2)$ 满足 $0 < c_i < \mathrm{e}^{a_i}$,

$$c_1 = (c_2 \cdots c_{r_1+r_2})^{-1} \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

构造凸闭集

$$B = \left\{(x_1, \cdots, x_n) \in \mathbb{R}^n \,\middle|\, |x_i| < c_i \ (1 \leqslant i \leqslant r_1), x_j^2 + x_{j+r_2}^2 \leqslant 2c_j \ (r_1+1 \leqslant j \leqslant r_1+r_2)\right\},$$

容易计算

$$\mu(B) = 2^{r_1+r_2}\pi^{r_2} c_1 \cdots c_{r_1+r_2} = 2^n \sqrt{|\Delta_K|} = 2^n \cdot d(\sigma(O_K)).$$

由 Minkowski 定理 (定理 13.4) 知存在 $\beta \in O_K$, 使得

$$0 \neq \sigma(\beta) \in B \cap \sigma(O_K),$$

由此可得 $|\beta^{(i)}| < c_i$, $1 \leqslant i \leqslant r_1$, $2\mathrm{Re}(\beta^{(i)})^2 + 2\mathrm{Im}(\beta^{(i)})^2 < 2c_i$, 即

$$|\beta^{(i)}|^2 < c_i, \quad r_1 + 1 \leqslant i \leqslant r_1 + r_2,$$

故对 $2 \leqslant i \leqslant r_1 + r_2$, 推得

$$b_i = \lambda_i \log|\beta^{(i)}| < \log c_i < a_i,$$

且

$$|N(\beta)| < c_1 \cdots c_{r_1+r_2} = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|},$$

证毕.

引理 6.8　*对任意* $k \in \{1, \cdots, r_1 + r_2\}$, *一定存在* $u_k \in U_K$, *设* $\ell(u_k) = (y_1, \cdots, y_{r_1+r_2})$, *使得对任意* $i \neq k$ *有* $y_i < 0$.

证明　记 $(\ell(\alpha))_i$ 表示 $\ell(\alpha)$ 的第 i 个分量, 取 $\alpha_1 \in O_K$, 重复利用引理 6.7 可知, 存在 O_K 中的一个序列 $\{\alpha_j\}_{j\geqslant 1}$ 使得

$$(\ell(\alpha_{j+1}))_i < (\ell(\alpha_j))_i, \quad i \neq k, \quad j \geqslant 1,$$

且

$$|N(\alpha_{j+1})| \leqslant \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

故 $N(\alpha_{j+1}O_K) \leqslant \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$ $(j \geqslant 1)$.

由定理 6.5 的证明可知, 理想集 $\{\alpha_j O_K\}_{j\geqslant 1}$ 是有限集, 因此存在 $j > h$ 使得 $\alpha_j O_h = \alpha_h O_K$, 即存在 $u_k \in U_K$, 使得 $\alpha_j = \alpha_h u_k$. 于是 $(\ell(\alpha_j))_i = (\ell(\alpha_h))_i + (\ell(u_k))_i$, 故对 $i \neq k$, 有 $(\ell(u_k))_i < 0$, 证毕.

引理 6.9 设 $u_1, \cdots, u_{r_1+r_2}$ 是引理6.8中所获得的元素组, 那么 $\{\ell(u_1), \cdots, \ell(u_{r_1+r_2})\}$ 的维数为 r_1+r_2-1.

证明 设 $\ell(u_i) = (a_{i,1}, \cdots, a_{i,r_1+r_2})$, 矩阵 $A = (a_{i,j})_{1\leqslant i,j\leqslant r_1+r_2}$, 除了对角线上元素为正, 其他全为负数, 且每行之和为 0, 这样的矩阵秩一定为 r_1+r_2-1. 设 A_i 为矩阵 A 的列向量 $1 \leqslant i \leqslant r_1+r_2$, 若 $\operatorname{rank}(A) \leqslant r_1+r_2-2$, 则 $A_1, \cdots, A_{r_1+r_2-1}$ 线性相关, 存在不全为零的实数 a_i, 使得

$$\sum_{i=1}^{r_1+r_2-1} a_i A_i = 0.$$

选 i_0 是集合 $\{|a_i| \mid 1 \leqslant i \leqslant r_1+r_2-1\}$ 中最大值的下角标, 那么存在 $|t_i| \leqslant 1$, $i \neq i_0$, $1 \leqslant i \leqslant r_1+r_2-1$, 使得

$$A_{i_0} + \sum_{i=1, i\neq i_0}^{r_1+r_2-1} t_i A_i = 0,$$

考虑第 i_0 个分量得

$$0 = a_{i_0,i_0} + \sum_{i=1,i\neq i_0}^{r_1+r_2-1} t_i a_{i_0,i} \geqslant a_{i_0,i_0} + \sum_{i=1,i\neq i_0}^{r_1+r_2-1} a_{i_0,i} > \sum_{i=1}^{r_1+r_2} a_{i_0,i} = 0.$$

矛盾, 证毕.

定理 6.8(Dirichlet 定理) $U_K \simeq W_K \times Z^r$, 其中 $r = r_1+r_2-1$.

F_K 的一组基称作 K 的一组基本单位系, 构造基本单位系是算法数论中一个很感兴趣的问题. 由上述引理 6.8 所得的 u_k 是通过一簇 O_K 中满足下列条件 (1)(2)(3) 来获得的序列 $\{\alpha_{k,j}\}_{j\in N}$:

(1) $\alpha_{k,1}$ 可以是 O_K 中任一非零元, 常取 $\alpha_{k,1} = 1$;

(2) $|\alpha_{k,j+1}^{(i)}| < |\alpha_{k,j}^{(i)}|, i \neq k; |\alpha_{k,j+1}^{(k)}| \geqslant |\alpha_{k,j}^{(k)}|$;

(3) $|N(\alpha_{k,j+1})| \leqslant C$, C 是某个常数.

而 $\alpha_{k,j}$ 是由 Minkowski 定理的存在性结论得到的. 因此我们希望寻找具体构造出 $\{\alpha_{k,j}\}$ 的方法, 用简单的替换, 令 $\beta_{k,j+1}=\dfrac{\alpha_{k,j+1}}{\alpha_{k,j}}$, 即等价去构造 $\{\beta_{k,j}\}$ 满足

(1)′ $\beta_{k,1}=1$;

(2)′ $\left|\beta_{k,j+1}^{(i)}\right|<1,\ i\neq k$; $\left|\beta_{k,j+1}^{(k)}\right|\geqslant 1,\ j\geqslant 1$;

(3)′ $\prod\limits_{i=1}^{j+1}\left|N(\beta_{k,i})\right|\leqslant C$.

我们用格基约化算法 (见 13.2 节) 去处理比这更一般化的问题.

设 $R=O_K$, $I=\{i_1,\cdots,i_\mu\}\subseteq\{1,\cdots,r_1+r_2\}$, $\tilde{I}=I\cup\{r_2+i_\nu\mid i_\nu>r_1,\ 1\leqslant\nu\leqslant\mu\}$, $|\tilde{I}|=\tilde{\mu}$, $J=\{1,\cdots,r_1+r_2\}\backslash I$, $\tilde{J}=\{1,\cdots,n\}\backslash\tilde{I}$. 希望递归地构造 R 上元素序列 $\{\beta_{I,k}\}_{k\geqslant 1}$ 和 n 维自由模序列 $\{M_{I,k}\}_{k\geqslant 1}$,

$$\beta_{I,1}=1,\quad M_{I,1}=R.$$

对 $k\geqslant 1$, $\beta_{I,k+1}\in M_{I,k}$, $M_{I,k+1}=\dfrac{1}{\beta_{I,k+1}}M_{I,k}$, 且满足

(1) $\left|\beta_{I,k+1}^{(j)}\right|<1,\ j\in\tilde{I}$, $\left|\beta_{I,k+1}^{(j)}\right|\geqslant 1,\ j\in\tilde{J}$;

(2) $\prod\limits_{i=0}^{k+1}|N(\beta_{I,i})|\leqslant\tilde{C}$(常数).

具体构造 $\beta_{I,k+1}$ 之前, 令 $r_{I,0}=1$, $r_{I,k+1}=\beta_{I,k+1}r_{I,k}$, 那么

$$M_{I,k+1}=t\frac{r_{I,k}}{r_{I,k+1}}M_{I,k}=\cdots=\frac{r_{I,1}}{r_{I,k+1}}M_{I,1}=\frac{1}{r_{I,k+1}}R.$$

令 $d\geqslant 1$ 是一个常数 (待定),

$$\lambda_j=\begin{cases}d, & j\in\tilde{J},\\ d^{1-\frac{n}{\mu}}, & j\in\tilde{I},\end{cases}$$

显然 $\prod\limits_{j=1}^{n}\lambda_j=1$, 定义 K 上的一个双线性型

$$\langle x,y\rangle_{\overline{\lambda}}=\sum_{j=1}^{n}\lambda_j^{-2}x^{(j)}\cdot\overline{y^{(j)}},$$

其对应的正定二次型为

$$L_{\overline{\lambda}}(x)=\sum_{j=1}^{n}\lambda_j^{-2}|x^{(j)}|^2.$$

取 R 的一组基 $\alpha_1,\cdots,\alpha_n$, 那么 $\left\{\omega_i=\dfrac{\alpha_i}{r_{I,k}}\right\}_{1\leqslant i\leqslant n}$ 便是自由 $\mathbb{Z}$-模 $M_{I,k}$ 的一组基. 定义嵌入映射 σ

$$\begin{aligned}\sigma_{\overline{\lambda}}: M_{I,k} &\longrightarrow \mathbb{R}^n,\\ \alpha &\longmapsto \big(\lambda_1^{-1}\alpha^{(1)},\cdots,\lambda_{r_1}^{-1}\alpha^{(r_1)},\sqrt{2}\lambda_{r_1+1}^{-1}\mathrm{Re}(\alpha^{(r_1+1)}),\cdots,\sqrt{2}\lambda_{r_1+r_2}^{-1}\mathrm{Re}(\alpha^{(r_1+r_2)}),\\ &\qquad \sqrt{2}\lambda_{r_1+r_2+1}^{-1}\mathrm{Im}(\alpha^{(r_1+1)}),\cdots,\sqrt{2}\lambda_{r_1+2r_2}^{-1}\mathrm{Im}(\alpha^{(r_1+r_2)})\big).\end{aligned}$$

$\sigma_{\overline{\lambda}}$ 满足 $\left|\left|\sigma_{\overline{\lambda}}(\alpha)\right|\right|^2=L_{\overline{\lambda}}(\alpha)$, 且 $\mathbb{R}^n$ 中格 $\sigma_{\overline{\lambda}}(M_{I,k})$ 的判别式

$$d\left(\sigma_{\overline{\lambda}}(M_{I,k})\right)=\left(\prod_{i=1}^{n}\lambda_i^{-1}\right)d\big(\sigma(M_{I,k})\big)=\frac{d(\sigma(R))}{|N(r_{I,k})|}=\frac{\sqrt{|\Delta_K|}}{|N(r_{I,k})|}.$$

取 $\beta_{I,k+1}$ 是格 $\sigma_{\overline{\lambda}}(M_{I,k})$ 的一组 LLL 约化基的第一个元素在 $M_{I,k}$ 中的逆象 β_1, 由约化基的性质知

$$L_{\overline{\lambda}}(\beta_1)=\left\|\sigma_{\overline{\lambda}}(\beta_1)\right\|^2\leqslant 2^{\frac{(n-1)}{2}}\left(\frac{\sqrt{|\Delta_K|}}{|N(r_{I,k})|}\right)^{\frac{2}{n}}.$$

令 $\hat{c}=2^{\frac{(n-1)}{4}}\left(\sqrt{|\Delta_K|}\right)^{\frac{1}{n}}$, 因为对任意 $1\leqslant j\leqslant n$, $L_{\overline{\lambda}}(\beta_1)\geqslant\left(\lambda_j^{-1}|\beta_1^{(j)}|\right)^2$, 所以

$$\left|\beta_1^{(j)}\right|\leqslant\lambda_j L_{\overline{\lambda}}(\beta_1)^{\frac{1}{2}}\leqslant\begin{cases}d^{1-\frac{n}{\tilde{\mu}}}\hat{c}|N(r_{I,k})|^{-\frac{1}{n}}, & j\in\tilde{I},\\ d\hat{c}|N(r_{I,k})|^{-\frac{1}{n}}, & j\in\tilde{J}.\end{cases}$$

从而

$$|N(\beta_1)|\leqslant\hat{c}^{\tilde{\mu}}|N(r_{I,k})|^{-\frac{\tilde{\mu}}{n}}d^{-(n-\tilde{\mu})}d^{n-\tilde{\mu}}\hat{c}^{n-\tilde{\mu}}|N(r_{I,k})|^{-\frac{n-\tilde{\mu}}{n}}=\hat{c}^n|N(r_{I,k})|^{-1}.$$

令 $\tilde{c}=\hat{c}^n$, $\beta_{I,k+1}$ 便满足 $(2)'$. 又因为 $|N(\beta_1)|\geqslant\dfrac{1}{|N(r_{I,k})|}$, 所以对 $j\in\tilde{J}$,

$$\left|\beta_1^{(j)}\right|=\frac{|N(\beta_1)|}{\prod\limits_{i\neq j}|\beta_1^{(i)}|}\geqslant\frac{|N(r_{I,k})|^{-1}}{\hat{c}^{(n-1)}d^{-1}|N(r_{I,k})|^{\frac{1}{n}-1}}=\hat{c}^{1-n}d|N(r_{I,k})|^{-\frac{1}{n}}.$$

假若选择 d 满足

$$d^{1-\frac{n}{\tilde{\mu}}}\hat{c}|N(r_{I,k})|^{-\frac{1}{n}}<1,\quad d\hat{c}^{1-n}|N(r_{I,k})|^{-\frac{1}{n}}\geqslant 1,$$

于是

$$d\geqslant\max\left\{\hat{c}^{n-1}|N(r_{J,k})|^{\frac{1}{n}},(\hat{c}|N(r_{I,k})|^{-\frac{1}{n}})^{\frac{\tilde{\mu}}{n-\tilde{\mu}}}\right\}=\hat{c}^{n-1}|N(r_{I,k})|^{\frac{1}{n}},$$

即可保证 $\beta_{I,k+1}$ 满足 $(1)'$, 从而由 $\{\beta_{I,k}\}_{k\geqslant 1}$, 可得出一个 U_K 的可逆元, 特别地，取

$$I=\{1,2,\cdots,n\}\backslash\{k\},$$

便构造出了满足引理 6.8 的 u_k.

W_K 的计算相对 F_K 的一组基本单位系的计算来说是容易的, W_K 是一个有限循环群 (见习题 6.16). 对任意 $x\in O_K$, 有不等式

$$L(x)=\sum_{i=1}^{n}|\sigma_i(x)|^2\geqslant n(|N(x)|)^{\frac{2}{n}}\geqslant n,$$

而上述等号成立当且仅当 $|N(x)|=1$, 且 $|\sigma_i(x)|=|\sigma_j(x)|$ 对任意 $1\leqslant i,j\leqslant n$. 故等价于 $|\sigma_i(x)|=1$, $1\leqslant i\leqslant n$, 即 $x\in W_K$. 也就是说, W_K 中的元素是格 (O_K,L) 中最短长度的向量.

设 $O_K=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$, $A=(\langle\alpha_i,\alpha_j\rangle)_{1\leqslant i,j\leqslant n}$, $x=(\alpha_1,\cdots,\alpha_n)(x_1,\cdots,x_n)^{\mathrm{T}}$, 以后将 x 和其在 $\alpha_1,\cdots,\alpha_n$ 表示下的坐标不加区别, 即 $x=(x_1,\cdots,x_n)^{\mathrm{T}}$, 那么 $L(x)=x^{\mathrm{T}}Ax$ 是一个正定二次型. 由线性代数理论可知, 存在一个矩阵 $Q=(q_{ij})_{1\leqslant i,j\leqslant n}$,

$$q_{ij}=\begin{cases}0, & i>j,\\ \sqrt{p_{ii}}, & i=j,\\ \sqrt{p_{ii}}p_{ij}, & i>j,\end{cases}$$

使得 $A=Q^{\mathrm{T}}Q$(见习题 6.17).

此时, $L(x)=\sum\limits_{i=1}^{n}p_{ij}\cdot\left(x_i+\sum\limits_{j=i+1}^{n}p_{ij}x_j\right)^2$, 这样, 用一簇不等式

$$p_{ii}\left(x_i+\sum_{j=i+1}^{n}p_{ij}x_j\right)^2\leqslant n-\sum_{k=i+1}^{n}p_{kk}\left(x_k+\sum_{j=k+1}^{n}p_{kj}x_j\right)^2,$$

从 n 起, 可以重复递归求出 $(x_1,\cdots,x_n)$ 的所有整数解, 因而得到 W_K 中的所有元素.

6.3 阶的一些性质

用 6.2 节讨论对 O_K 的一个非零素理想 $\mathfrak{p}$, 有 p-adic 赋值 $\nu_{\mathfrak{p}}$, 现讨论对一般的阶 A, 寻找和 $\nu_{\mathfrak{p}}$ 类似的同态映射.

引理 6.10 对 A 的任一非零素理想 $\mathfrak{p}$ 一定存在一个群同态 $\ell_{\mathfrak{p}}: K^* \longrightarrow \mathbb{Z}$ 且满足

(1) $\ell_{\mathfrak{p}}(x) \geqslant 0$ 对所有 $x \in A, x \neq 0$;

(2) $0 \neq x \in A$, 那么 $\ell_{\mathfrak{p}}(x) > 0$ 当且仅当 $x \in \mathfrak{p}$;

(3) 任意 $x \in K^*$, 几乎对所有 A 的素理想 $\mathfrak{p}$(除了有限个外) 均有 $\ell_{\mathfrak{p}}(x) = 0$ 且

$$\prod_{\mathfrak{p}} N(\mathfrak{p})^{\ell_{\mathfrak{p}}(x)} = |N(x)|,$$

$\mathfrak{p}$ 跑遍 A 的所有素理想.

为了证明引理 6.10, 引入一个重要的定理.

定理 6.9 (Jordan-Hölder定理) 模 M 的任两个复合链都是等价的, 即模 M 的任两个复合链导出的各自因子模是一一对应且是同构的.

引理 6.10 的证明 对任 $0 \neq x \in A$, 因为 $[A : xA] < +\infty$, 任意取一个关于 x 的理想复合链

$$A = \mathfrak{a}_0 \supsetneqq \mathfrak{a}_1 \supsetneqq \cdots \supsetneqq \mathfrak{a}_{t-1} \supsetneqq \mathfrak{a}_t = xA,$$

即在 $\mathfrak{a}_{i-1}$ 和 $\mathfrak{a}_i$ 之间没有非平凡的理想 $(1 \leqslant i \leqslant t)$, 定义

$$\ell_{\mathfrak{p}}(x) = \left|\left\{i \in \{1, 2, \cdots, t\} \middle| \frac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i} \cong A/\mathfrak{p}\right\}\right|.$$

由 Jordan-Hölder 定理可知 $\ell_{\mathfrak{p}}(x)$ 和复合链的选取是无关的, 对 $y \in A$, 设

$$A = \mathfrak{b}_0 \supsetneqq \mathfrak{b}_1 \supsetneqq \cdots \supsetneqq \mathfrak{b}_{s-1} \supsetneqq \mathfrak{b}_s = yA$$

是关于 y 的复合链, 显然

$$A = \mathfrak{a}_0 \supsetneqq \cdots \supsetneqq \mathfrak{a}_t = xA = x\mathfrak{b}_0 \supsetneqq \cdots \supsetneqq x\mathfrak{b}_s = xyA$$

是关于 xy 的复合链, 故

$$\ell_{\mathfrak{p}}(xy) = \ell_{\mathfrak{p}}(x) + \ell_{\mathfrak{p}}(y).$$

自然扩展 $\ell_{\mathfrak{p}}$, 对 $x/z \in K^*$, 定义

$$\ell_{\mathfrak{p}}(x/z) = \ell_{\mathfrak{p}}(x) - \ell_{\mathfrak{p}}(z),$$

那么 $\ell_{\mathfrak{p}}$ 是 $K^* \longrightarrow \mathbb{Z}$ 的一个群同态, (1) 得证.

(2) 若 $x \in \mathfrak{p}$, 取理想链 $A = \mathfrak{a}_0 \supseteq \mathfrak{a}_1 = \mathfrak{p} \supseteq xA$, 由于任意理想链都可扩充成一个复合链, 故 $\ell_{\mathfrak{p}}(x) \geqslant 1$.

若 $x \notin \mathfrak{p}$, 因为 $\mathfrak{p}$ 是极大理想, 所以 $\mathfrak{p} + xA = A$, 于是存在 $z \in \mathfrak{p}$, 满足 $z \equiv 1(\mathrm{mod} xA)$, 更一般地,

$$z \equiv 1(\mathrm{mod} \mathfrak{a}_i), \quad 1 \leqslant i \leqslant t,$$

因此

$$z \cdot \left(\frac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i}\right) = \frac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i},$$

故 $\dfrac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i}$ 不可能同构 $A/\mathfrak{p}$, 此时 $\ell_{\mathfrak{p}}(x) = 0$.

(3) 显然只需证对 $x \in A$ 结论成立即可. 首先证明: 对任意 $1 \leqslant i \leqslant t$, 一定存在唯一素理想 $\mathfrak{p} \subseteq A$ 使得 $\dfrac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i} \cong A/\mathfrak{p}$. 取 $y \in \mathfrak{a}_{i-1} - \mathfrak{a}_i$, 那么

$$\mathfrak{a}_i + yA = \mathfrak{a}_{i-1},$$

故 y 诱导出一个 A-模满同态

$$\begin{aligned} \varphi : A &\longrightarrow \frac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i} \\ z &\longmapsto yz \,(\mathrm{mod}\ \mathfrak{a}_i). \end{aligned}$$

因此 $A/\ker\varphi \cong \mathfrak{a}_{i-1}/\mathfrak{a}_i$, 令 $\mathfrak{p} = \ker\varphi$, 因为 $\mathfrak{a}_{i-1}/\mathfrak{a}_i$ 是不可约 A-模, 所以 $\mathfrak{p}$ 是极大理想. 事实上, $\mathfrak{p}$ 是 A-模 $\mathfrak{a}_{i-1}/\mathfrak{a}_i$ 的零化子, 故由 $\mathfrak{a}_{i-1}/\mathfrak{a}_i$ 唯一确定, 和 y 的选取无关. 因此

$$|N(x)| = |A/xA| = \prod_{i=1}^{t} \left|\frac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i}\right| = \prod_{\mathfrak{p}} N(\mathfrak{p})^{\ell_{\mathfrak{p}}(x)},$$

证毕.

映射 $\ell_{\mathfrak{p}}$ 是由引理 6.10 中的条件 (1)(2)(3) 所唯一确定的 (见习题 6.18).

当取 $A = O_K$ 时, 对 $x \in O_K$, 有

$$xO_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \quad \mathfrak{p}_i\text{是素理想}, e_i \geqslant 1, \tag{$\star$}$$

对 O_K 的非零素理想 $\mathfrak{p}$, 定义 $\nu_{\mathfrak{p}}(x)$ 为 xO_K 如上 ($\star$) 的表示式中 $\mathfrak{p}$ 出现的个数 (重数), 对 $x/z \in K^*$, 其中 $x, z \in O_K$, 自然扩充 $\nu_{\mathfrak{p}}(x/z) = \nu_{\mathfrak{p}}(x) - \nu_{\mathfrak{p}}(z)$. 由中国剩余定理和结论 $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$(见习题 6.19) 知, $\nu_{\mathfrak{p}}$ 也满足引理 6.10 中的条件 (1)(2)(3),

由唯一性可知 $\nu_{\mathfrak{p}}=\ell_{\mathfrak{p}}$. 事实上, 若设 $xO_K=\mathfrak{p}_1\cdots\mathfrak{p}_t$($\mathfrak{p}_i$ 允许相同), 取 $\mathfrak{a}_i=\mathfrak{p}_1\cdots\mathfrak{p}_i$, $1\leqslant i\leqslant t$, 便可得复合链

$$O_K=\mathfrak{a}_0\supsetneqq\mathfrak{p}_1\supsetneqq\mathfrak{p}_1\mathfrak{p}_2\supsetneqq\cdots\supsetneqq\mathfrak{p}_1\cdots\mathfrak{p}_t=xO_K,$$

且

$$\frac{\mathfrak{a}_{i-1}}{\mathfrak{a}_i}\cong O_K/\mathfrak{p}_i.$$

令 A,B 都是 K 的阶, 且 $A\subseteq B$, 对 B 的任一个非零素理想 $\mathfrak{P}$, $\mathfrak{P}\cap A=\mathfrak{p}$ 为 A 的非零素理想, 以后记 $\mathfrak{P}|\mathfrak{p}$, 且 $B/\mathfrak{P}$ 是 $A/\mathfrak{p}$ 的一个有限扩张, 用 $f(\mathfrak{P}|\mathfrak{p})$ 记作此扩张的次数, 为了防止符号混淆, 下面用 $\ell_{\mathfrak{p},A}$ 来记上面讨论时用的 $\ell_{\mathfrak{p}}$.

引理 6.11 令 $\mathfrak{p}$ 是 A 的一个非零素理想, x 是 K 中非零元素, 那么

$$\ell_{\mathfrak{p},A}(x)=\sum_{\mathfrak{P}|\mathfrak{p}}f(\mathfrak{P}|\mathfrak{p})\ell_{\mathfrak{P},B}(x).$$

证明 为方便起见, 引入一个记号, 设 M 是一个有限 A-模, 记 $\ell_{\mathfrak{p},A}(M)$ 为 M 的同构 $A/\mathfrak{p}$ 的复合因子的个数, 那么 $\ell_{\mathfrak{p},A}(x)=\ell_{\mathfrak{p},A}(A/xA)$, 另外, 对 M 的一个子模 L, 显然有

$$\ell_{\mathfrak{p},A}(M)=\ell_{\mathfrak{p},A}(L)+\ell_{\mathfrak{p},A}(M/L).$$

注意到, 对任意非零元 $x\in A$, A-模 B/A 和 xB/xA 是同构的, 因此

$$\begin{aligned}&\ell_{\mathfrak{p},A}(B/A)=\ell_{\mathfrak{p},A}(xB/xA),\\&\ell_{\mathfrak{p},A}(x)=\ell_{\mathfrak{p},A}(A/xA)=\ell_{\mathfrak{p},A}(B/xA)-\ell_{\mathfrak{p},A}(B/A)\\&\qquad\quad=\ell_{\mathfrak{p},A}(B/xA)-\ell_{\mathfrak{p},A}(xB/xA)=\ell_{\mathfrak{p},A}(B/xB).\end{aligned}$$

令 $M=B/xB$, 只需证

$$\ell_{\mathfrak{p},A}(M)=\sum_{\mathfrak{P}|\mathfrak{p}}f(\mathfrak{P}|\mathfrak{p})\ell_{\mathfrak{P},B}(M).\tag{6.2}$$

下面证明对任意有限 B-模 M, 式 (6.2) 都成立. 通过选择 M 的一个复合链, 不妨假设 M 为 B-单模, 即只有 $\{0\}$, M 作为 M 的子模, 显然, $M\cong B/\mathfrak{P}'$, 其中 $\mathfrak{P}'$ 是 B 的极大理想, 且

$$\ell_{\mathfrak{P},B}(M)=\begin{cases}1, & \mathfrak{P}'=\mathfrak{P}',\\0, & \mathfrak{P}\neq\mathfrak{P}'.\end{cases}\tag{6.3}$$

令 $\mathfrak{p}'=\mathfrak{P}'\cap A$, 而 $M=B/\mathfrak{P}'$ 看成 A-模和看成 $A/\mathfrak{p}'$-模有相同的结构, 故 M 是 $f(\mathfrak{P}'|\mathfrak{p}')$ 个 $A/\mathfrak{p}'$ 的直和.

$$\ell_{\mathfrak{p},A}(M)=\begin{cases}f(\mathfrak{P}'|\mathfrak{p}'), & \mathfrak{p}=\mathfrak{p}',\\0, & \mathfrak{p}\neq\mathfrak{p}',\end{cases}\tag{6.4}$$

综合式 (6.3), 式 (6.4) 可知式 (6.2) 成立, 证毕.

上述性质表明, 对 A 中的任一素理想 $\mathfrak{p}$, 有且只有有限个由 $\mathfrak{p}$ 提升到 B 的素理想 $\mathfrak{P}$, 即 $\mathfrak{P}|\mathfrak{p}$. 事实上, 除有限个 $\mathfrak{p}$ 之外, 其他的素理想能且只能提升成 B 的一个素理想.

引理 6.12 *A 中除有限个素理想外, 均有*

$$\sum_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p}) = 1,$$

且整数

$$\prod_{\mathfrak{p}} N(\mathfrak{p})^{-1+\sum\limits_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})} \,\Big|\, [B:A],$$

其中 $\mathfrak{p}$ 跑遍 A 的所有素理想.

证明 取 T 是 A 中的任意有限个素理想构成的集合, U 是由 T 中的素理想提升到 B 中的素理想全体. 令 $\mathfrak{a} = \bigcap\limits_{\mathfrak{p}\in T} \mathfrak{p}, \mathfrak{b} = \bigcap\limits_{\mathfrak{P}\in U} \mathfrak{P}$, 那么 $\mathfrak{a} = \mathfrak{b} \cap A$. 将 $A/\mathfrak{a}$ 看成 $B/\mathfrak{b}$ 的子环, 因为

$$[B:\mathfrak{b}][\mathfrak{b}:\mathfrak{a}] = [B:\mathfrak{a}] = [B:A][A:\mathfrak{a}],$$

即

$$[B:A] = \frac{[B:\mathfrak{b}]}{[A:\mathfrak{a}]} \cdot [\mathfrak{b}:\mathfrak{a}] = [B/\mathfrak{b}:A/\mathfrak{a}][\mathfrak{b}:\mathfrak{a}],$$

故 $[B/\mathfrak{b}:A/\mathfrak{a}] \mid [B:A]$. 由中国剩余定理知

$$A/\mathfrak{a} \cong \prod_{\mathfrak{p}\in T} A/\mathfrak{p},$$

$$B/\mathfrak{b} \cong \prod_{\mathfrak{P}\in U} B/\mathfrak{P},$$

$$|A/\mathfrak{a}| = \prod_{\mathfrak{p}\in T} N(\mathfrak{p}),$$

$$|B/\mathfrak{b}| = \prod_{\mathfrak{P}\in U} N_B(\mathfrak{P}) = \prod_{\mathfrak{p}\in T} N(\mathfrak{p})^{\sum\limits_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})}.$$

于是

$$[B/\mathfrak{b}:A/\mathfrak{a}] = \prod_{\mathfrak{p}\in T} N(\mathfrak{p})^{-1+\sum\limits_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})} \Big| [B:A].$$

由 T 的任意性可知, A 中满足 $\sum\limits_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p}) \neq 1$ 的素理想只有有限多个, 取 T 为这些素理想构成的集合, 便证明本命题.

记 $\vee_A = \{x \in K^* |\ \ell_{\mathfrak{p},A}(x) \equiv 0 \pmod 2$, 对所有 A 的素理想 $\mathfrak{p}\}$.

引理 6.13 若 $A\subseteq B$ 是 K 的阶, 那么 $\vee_B\subseteq\vee_A$, 且

$$[\vee_A:\vee_B]\leqslant[B:A].$$

证明 由引理 6.11 和 $\vee_A$ 的定义可知, $\vee_B\subseteq\vee_A$. 对 A 的每个非零素理想 $\mathfrak{p}$, 定义

$$S_{\mathfrak{p}}=\begin{cases}\{\mathfrak{P}|\ \mathfrak{P}\text{是}B\text{的素理想},\mathfrak{P}|\mathfrak{p}\}, & f(\mathfrak{P}/\mathfrak{p})\text{是偶数, 对所有}\mathfrak{P}|\mathfrak{p},\\ \{\mathfrak{P}|\ \mathfrak{P}\text{是}B\text{的素理想},\mathfrak{P}|\mathfrak{p}\}-\{\mathfrak{P}_0\}, & \text{存在}\mathfrak{P}_0|\mathfrak{p},\text{使}f(\mathfrak{P}_0/\mathfrak{p})\text{是奇数}.\end{cases}$$

由 $S_{\mathfrak{p}}$ 的构造, 自然对所有 $\mathfrak{p}$,

$$|S_{\mathfrak{p}}|\leqslant-1+\sum_{\mathfrak{P}|\mathfrak{p}}f(\mathfrak{P}/\mathfrak{p}).$$

由引理 6.12 知, 几乎对所有 $\mathfrak{p}$, $S_{\mathfrak{p}}=\varnothing$, 令 $S=\bigcup\limits_{\mathfrak{p}}S_{\mathfrak{p}}$ 是有限集, $s=|S|$, 则

$$2^s\leqslant\prod_{\mathfrak{p}}N(\mathfrak{p})^{|S_{\mathfrak{p}}|}\leqslant\prod_{\mathfrak{p}}N(\mathfrak{p})^{-1+\sum\limits_{\mathfrak{P}|\mathfrak{p}}f(\mathfrak{P}/\mathfrak{p})}\leqslant[B:A].$$

下面只需证明, 群 $\vee_A/\vee_B$ 能够嵌入到 $(\mathbb{Z}/2\mathbb{Z})^s$ 中即可, 令

$$\begin{aligned}\varphi:\vee_A&\longrightarrow(\mathbb{Z}/2\mathbb{Z})^s,\\ x&\longmapsto(\ell_{\mathfrak{P},B}(x)\,(\mathrm{mod}\ 2))_{\mathfrak{P}\in S}\end{aligned}$$

是一个群同态, $x\in\ker(\varphi)$ 当且仅当对所有 $\mathfrak{P}\in S$, $\ell_{\mathfrak{P},B}(x)\equiv0(\mathrm{mod}2)$. 对任意 $\mathfrak{P}'\notin S$, 记 $\mathfrak{p}'=\mathfrak{P}'\cap A$, 那么 $S_{\mathfrak{p}'}=\varnothing$, 即 $f(\mathfrak{P}'|\mathfrak{p}')=1$, 且 $\mathfrak{p}'$ 有且只有 $\mathfrak{P}'$, 使 $\mathfrak{P}'|\mathfrak{p}'$, 那么

$$\ell_{\mathfrak{p}',A}(x)=\sum_{\mathfrak{P}|\mathfrak{p}'}f(\mathfrak{P}|\mathfrak{p}')\ell_{\mathfrak{P},B}(x)=\ell_{\mathfrak{P}',B}(x)\equiv0\,(\mathrm{mod}\ 2),$$

所以 $x\in\vee_B$, 因而 $\ker\varphi=\vee_B$, 证毕.

习　题

习题 6.1 记 $\{\theta_i\}_{1\leqslant i\leqslant n}$ 是 n 次多项式 $f(x)$ 在复数域 $\mathbb{C}$ 上的所有根, $\Delta(f)$ 和 $\mathrm{res}\,(f,f')$ 的定义同 6.1 节, 试证

$$\Delta(f)=\prod_{1\leqslant i<j\leqslant n}(\theta_i-\theta_j)^2=(-1)^{\frac{n(n-1)}{2}}N(f'(\theta))=(-1)^{\frac{n(n-1)}{2}}\mathrm{res}\,(f,f').$$

习题 6.2 若 L 是 $K/\mathbb{Q}$ 的中间域, 试证 $N_{K/L}$ 和 $T_{K/L}$ 满足

(1) 对任意 $\alpha, \beta \in K$, $N_{K/L}(\alpha\beta) = N_{K/L}(\alpha)N_{K/L}(\beta), T_{K/L}(\alpha+\beta) = T_{K/L}(\alpha) + T_{K/L}(\beta)$;

(2) 对于 $\alpha \in L$, $N_{K/L}(\alpha) = \alpha^d$, $T_{K/L}(\alpha) = d \cdot \alpha$, 其中 $d = [K : L]$;

(3) 设 $\mathbb{Q} \subseteq M \subseteq L \subseteq K$ 是数域链, 对于 $\alpha \in K$, $N_{K/M}(\alpha) = N_{L/M}\left(N_{K/L}(\alpha)\right)$, $T_{K/M}(\alpha) = T_{L/M}\left(T_{K/L}(\alpha)\right)$;

(4) $N(\alpha) = \prod\limits_{i=1}^{n} \sigma_i(\alpha)$, $T(\alpha) = \sum\limits_{i=1}^{n} \sigma_i(\alpha)$.

习题 6.3 设 $K = \mathbb{Q}(\theta) = \mathbb{Q}[x]/(f(x))$ 是 $\mathbb{Q}$ 上的一个 n 次扩张 ($f(x)$ 是 θ 的极小多项式, 且 $\deg f(x) = n$), σ_i 是 $K \longrightarrow K_i = \mathbb{Q}(\theta_i)$ 的同构映射, $1 \leqslant i \leqslant n$, 任取 $\alpha_1, \cdots, \alpha_n \in K$, 试证 $\{\alpha_1, \cdots, \alpha_n\}$ 是一组 $\mathbb{Q}$-基当且仅当 $d_K(\alpha_1, \cdots, \alpha_n) \neq 0$.

习题 6.4 证明: 对 $\mathbb{Q}$ 上任意一个有限扩张 K, 必定存在一个代数整数 θ, 满足 $K = \mathbb{Q}(\theta)$.

习题 6.5 证明: 对 $\mathbb{Q}$ 上任意一个有限扩张 K, K 中所有代数整数构成一个环.

习题 6.6 K 是 $\mathbb{Q}$ 上任意一个有限扩张, O_K 是 K 中所有代数整数构成的子环, 证明: $O_K \cap \mathbb{Q} = \mathbb{Z}$.

习题 6.7 $\alpha_1, \cdots, \alpha_n$ 是 K 的一组基, 并记 $A = (\langle \alpha_i, \alpha_j \rangle)_{1 \leqslant i,j \leqslant n}$. 若 $\alpha_1, \cdots, \alpha_n$ 均是代数整数, 证明 $\det(A) = |d_K(\alpha_1, \cdots, \alpha_n)| \in \mathbb{Z}$.

习题 6.8 $\sqrt{|\Delta(f)|} = \sqrt{|\Delta_K|}[O_K : \mathbb{Z}[\theta]]$.

习题 6.9 求二次域的整基.

习题 6.10 令 R 是一个含幺交换环. 证明下列条件是等价的:

(1) R 是 Noether 环;

(2) R 的理想升链一定有限, 即

$$A_1 \subseteq \cdots \subseteq A_n \subseteq \cdots$$

是 R 的理想链, 那么一定存在 $k \in \mathbb{N}$ 使得 $A_k = A_{k+1} = \cdots$;

(3) R 的任意一个由理想构成的非空集合一定有极大元.

习题 6.11 证明: 理想的范映射 N 一定满足

(1) $|N(x)| = N(xA)$, 特别地, $A = O_K$ 时, N 还满足

(2) $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$,

(3) $d_K(\mathfrak{a}) = N(\mathfrak{a})^2 \Delta_K$.

习题 6.12 证明 $d(\mathfrak{a}) = d\left(\sigma(\mathfrak{a})\right)^2$, 即理想 $\mathfrak{a}$ 的判别式等于格 $\sigma(\mathfrak{a})$ 的判别式的平方.

习题 6.13 记 h_K 是代数数域 K 的类数, 证明: $h_K=1\Leftrightarrow O_K$ 是主理想整环 $\Leftrightarrow O_K$ 是唯一分解整环.

习题 6.14 令 $\alpha\in O_K$, 证明

(1) $\alpha\in U_K\Leftrightarrow |N(\alpha)|=1$;

(2) $\alpha\in W_K\Leftrightarrow \forall 1\leqslant i\leqslant n, |\sigma_i(\alpha)|=1$.

习题 6.15 $\mathbb{R}^n$ 中的任一离散子群一定是 $\mathbb{R}^n$ 中某个 r $(0\leqslant r\leqslant n)$ 维子空间中的格.

习题 6.16 记 U_K 为 O_K 中所有可逆元构成的乘法群, W_K 是 U_K 的扭子群, 即 U_K 中的所有有限阶元 (此时即为单位根) 全体, 证明 W_K 必定是一个有限循环群.

习题 6.17 设 $O_K=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$, 试给出一个算法求矩阵 $Q=(q_{ij})_{1\leqslant i,j\leqslant n}$, 满足:

(1) $A=(\langle\alpha_i,\alpha_j\rangle)_{1\leqslant i,j\leqslant n}=Q^{\mathrm{T}}Q$;

(2) $q_{ij}=\begin{cases}0, & i>j,\\ \sqrt{p_{ii}}, & i=j,\\ \sqrt{p_{ii}}p_{ij}, & i>j.\end{cases}$

习题 6.18 对 A 的任一非零素理想 $\mathfrak{p}$ 一定存在唯一一个群同态 $\ell_{\mathfrak{p}}:K^*\longrightarrow\mathbb{Z}$, 满足

(1) $\ell_{\mathfrak{p}}(x)\geqslant 0$ 对所有 $x\in A, x\neq 0$;

(2) $0\neq x\in A$, 那么 $\ell_{\mathfrak{p}}(x)>0$ 当且仅当 $x\in\mathfrak{p}$;

(3) 任意 $x\in K^*$, 几乎对所有 A 的素理想 $\mathfrak{p}$(除了有限个外) 均有 $\ell_{\mathfrak{p}}(x)=0$ 且

$$\prod_{\mathfrak{p}}N(\mathfrak{p})^{\ell_{\mathfrak{p}}(x)}=|N(x)|,$$

$\mathfrak{p}$ 跑遍 A 的所有素理想.

习题 6.19 证明: $N(\mathfrak{p}^e)=N(\mathfrak{p})^e$.

第 7 章　椭 圆 曲 线

7.1　椭圆曲线的群结构

7.1.1　Weierstrass方程

设K为一个域, $\overline{K}$表示K的代数闭域. K上的Weierstrass 方程

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{7.1}$$

$(a_1, a_2, a_3, a_4, a_5, a_6 \in K)$ 决定射影平面 $\mathbb{P}^2(\overline{K})$ 上的一条曲线 E, 即适合上述方程的点 (X, Y, Z) $(X, Y, Z \in \overline{K})$ 的集合. 当该曲线非奇异时, 称它为定义在 K 上的椭圆曲线, 以 E/K 表示. 将方程 (7.1) 改写为形如 $F(X, Y, Z) = 0$ 的方程, E 为非奇异是指 E 上不存在奇点, 即 E 上不存在使 $\partial F/\partial X, \partial F/\partial Y$ 和 $\partial F/\partial Z$ 同时为零的点.

E 上有唯一的一个点 $(0, 1, 0)$, 具有坐标 $Z = 0$, 称该点为无穷远点, 记为 $\mathcal{O}$. 由于 $\partial F/\partial Z(\mathcal{O}) = 1$, 故 $\mathcal{O}$ 不是奇点. 当 $Z \neq 0$ 时, 令 $x = X/Z, y = Y/Z$, 方程 (7.1) 变为

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{7.2}$$

曲线 E 由方程 (7.2) 所有的解 (x, y) $(x, y \in \overline{K})$ 及无穷远点 $\mathcal{O}$ 组成. 将方程 (7.2) 表为 $f(x, y) = 0$ 的形式, E 上不存在使 $\partial f/\partial x$ 和 $\partial f/\partial y$ 同时为零的点. E 上的每个点 (无穷远点除外) 都有射影坐标 (X, Y, Z) 和仿射坐标 (x, y) 两种表示方式.

当 K 的特征 $\mathrm{char}(K) \neq 2$ 时, 以 $y - a_1x/2 - a_3/2$ 代入式 (7.2) 中的 y 得

$$E : y^2 = x^3 + b_2x^2/4 + b_4x/2 + b_4/4, \tag{7.3}$$

其中

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = 2a_4 + a_1a_3,$$

$$b_6 = a_3^2 + 4a_6.$$

当 $\mathrm{char}(K) \neq 2, 3$ 时, 在式 (7.3) 中再以 $x - b_2/12$ 代入 x 得

$$E : y^2 = x^3 + ax + b, \tag{7.4}$$

其中

$$a = -c_4/(3 \times 2^4), \quad b = -c_6/(3^3 \times 2^5),$$
$$c_4 = b_2^2 - 24b_4, \qquad c_6 = b_2^3 + 36b_2b_4 - 216b_6.$$

定义 E 的两个重要参数

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$
$$j = c_4^3/\Delta.$$

Δ 称为 E 的判别式, j 称为 E 的 j 不变量, 其中 $b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$.

E 上没有奇点, 故 $f(x) = x^3 + ax + b = 0$ 没有重点, 即 $f(x)$ 与 $f'(x)$ 的结式 $4a^3 + 27b^2 \neq 0$. 通过直接计算可知 $\Delta = -16(4a^3 + 27b^2)$, 可见 E 为非奇异的充要条件是 $\Delta \neq 0$.

当 $\mathrm{char}(K) = 3$ 时, 将方程 (7.3) 改写为

$$E: y^2 = x^3 + a_2 x^2 + a_4 x + a_6. \tag{7.5}$$

易见, 当且仅当 $\Delta = a_2^2 a_4^2 - a_2^3 a_6 - a_4^3 \neq 0$ 时, E 为非奇异. 若式 (7.5) 中 $a_2 = 0$, 则有

$$E: y^2 = x^3 + a_4 x + a_6, \quad \Delta = -a_4^3, \quad j = 0. \tag{7.6}$$

当 $a_2 \neq 0$ 时, 在式 (7.5) 中以 $x + a_4/a_2$ 代入 x, 式 (7.5) 化为

$$E: y^2 = x^3 + a_2 x^2 + a_6, \quad \Delta = -a_2^3 a_6, \quad j = -a_2^3/a_6 \tag{7.7}$$

(约定 a_i 可以代表不同的值).

当 $\mathrm{char}(K) = 2$ 时, 方程 (7.2) 中若 $a_1 \neq 0$, 分别以 $a_1^2 x + a_3/a_1$ 和 $a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3$ 代入 x 和 y, 式 (7.2) 化为

$$E: y^2 + xy = x^3 + a_2 x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6, \tag{7.8}$$

若式 (7.2) 中 $a_1 = 0$, 则以 $x + a_2$ 代入 x 得

$$E: y^2 + a_3 y = x^3 + a_4 x + a_6, \quad \Delta = a_3^4, \quad j = 0. \tag{7.9}$$

对于方程 (7.6)~(7.9) 定义的曲线, 可以分别验证当且仅当 $\Delta \neq 0$ 时, 它们为非奇异的.

7.1.2　椭圆曲线上的加法

方程 (7.1) 所定义的椭圆曲线 E 是射影平面 $\mathbb{P}^2(\overline{K})$ 上的一条 3 次曲线, 平面上任一直线与 E 都有三个交点 (不一定互不相同). 任取 E 上两点 P, Q, 连接 P, Q 的直线 (当 $P = Q$ 时, 取通过 P 的切线) 与 E 交于第三点 R, 将连接 R 与无穷远点 $\mathcal{O}$ 的直线与 E 的第三个交点记为 $P \oplus Q$. 在实数平面上, 上述过程如图 7.1 所示.

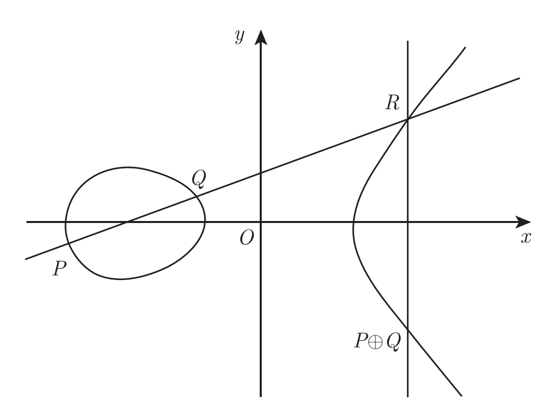


图 7.1　椭圆曲线上两个点的 $\oplus$ 运算

定理 7.1　运算 $\oplus$ 具有下述性质:

(1) 若直线 L 与 E 相交于 P, Q, R 三点, 则 $(P \oplus Q) \oplus R = \mathcal{O}$;

(2) 对任一 $P \in E$ 有 $P \oplus \mathcal{O} = P$;

(3) 对任一 $P, Q \in E$ 有 $P \oplus Q = Q \oplus P$;

(4) 对任一 $P \in E$, 存在 E 上一点, 表示为 $\ominus P$, 使 $P \oplus (\ominus P) = \mathcal{O}$;

(5) 设 $P, Q, R \in E$, 则 $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

换句话说, 运算 $\oplus$ 使 E 成为一个交换群, 以下称它为 E 上的加法群, 并将 $\oplus, \ominus$ 分别改写为 $+, -$.

证明　(1) 将方程 (7.1) 改写为形如 $F(X, Y, Z) = 0$, 易见 $\partial F/\partial X(\mathcal{O}) = 0, \partial F/\partial Y(\mathcal{O}) = 0$, $\partial F/\partial Z(\mathcal{O}) = 1$, E 与过 $\mathcal{O}$ 的切线 $Z = 0$ 有唯一的交点 $\mathcal{O}$(三重交点). 由 $\oplus$ 的定义, 通过 $P \oplus Q$ 与 R 的直线交 E 于 $\mathcal{O}$, 而通过 $\mathcal{O}$ 的切线与 E 的第三个交点仍是 $\mathcal{O}$, 所以 (1) 得证.

(2) 设 R 为通过 P 与 $\mathcal{O}$ 的连线与 E 的第三个交点, 则通过 R 与 $\mathcal{O}$ 的连线交 E 于 P, 即有 $P \oplus \mathcal{O} = P$.

(3) 在 $\oplus$ 的定义中, P 与 Q 是对称的.

(4) 将 P 与 $\mathcal{O}$ 的连线与 E 的第三个交点记为 R, 利用 (1) 与 (2), 有

$$\mathcal{O} = (P \oplus \mathcal{O}) \oplus R = P \oplus R,$$

即 $\ominus P = R$.

(5) 利用以下将推导的运算 $\oplus$ 的表达式, 可得到 $\oplus$ 的结合律. 定理 7.1 得证.

现在来推导 E 的加法运算表达式. 设定义 E 的方程为

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0, \tag{7.10}$$

$P = (x_0, y_0) \in E$, 首先来推导 $-P$ 的表达式. 通过 P 与 $\mathcal{O}$ 的直线 $L : x = x_0$, L 与 E 的第三个交点即为 $-P$. 将 $x = x_0$ 代入式 (7.10) 得到 y 的二次方程

$f(x_0,y)=0$, 它的两个解即对应 L 与 E 的两个交点 $P=(x_0,y_0)$ 及 $-P=(x_0,y_0')$, 可见 $y_0+y_0'=-a_1x_0-a_3$, 所以 $-P=(x_0,-y_0-a_1x_0-a_3)$.

设 $P_1=(x_1,y_1)$ 及 $P_2=(x_2,y_2)$ 为 E 上两点. 当 $x_1=x_2, y_1+y_2+a_1x_1+a_3=0$ 时, $P_1+P_2=\mathcal{O}$. 当 $P_1+P_2\neq\mathcal{O}$ 时, 通过 P_1 与 P_2 的直线形如

$$L: y=\lambda x+v.$$

若 $x_1\neq x_2$, 则 $\lambda=(y_1-y_2)/(x_1-x_2)$; 若 $x_1=x_2$, 由于 $P_1+P_2\neq\mathcal{O}$, 所以 $P_1=P_2, L$ 为过 P_1 的切线, $\lambda=-\dfrac{\partial f}{\partial x}(P_1)\Big/\dfrac{\partial f}{\partial y}(P_1)$, λ 确定后可得到 v. 记 L 与 E 的第三个交点为 $P_3=(x_3,y_3)$, 则 $P_1+P_2=-P_3$. 将 L 的方程代入式 (7.10) 得

$$f(x,\lambda x+v)=(x-x_1)(x-x_2)(x-x_3),$$

由 $x_1+x_2+x_3=\lambda^2+a_1\lambda-a_2$ 可计算出 x_3 和 y_3.

E **的加法规则** 设 E 为由方程 (7.10) 定义的椭圆曲线.

(a) 设 $P=(x,y)\in E$, 则 $-P=(x,-y-a_1x-a_3)$; 令

$$P_1+P_2=P_3,\quad P_i=(x_i,y_i)\in E,\quad i=1,2,3.$$

(b) 若 $x_1=x_2, y_1+y_2+a_1x+a_3=0$, 则 $P_1+P_2=\mathcal{O}$; 否则令

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & x_1\neq x_2,\\[2mm] \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & x_1=x_2,\end{cases}$$
$$v=y_1-\lambda x_1.$$

(c) P_3 由下式给出:

$$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2,$$
$$y_3=\lambda(x_1-x_3)-y_1-a_1x_3-a_3.$$

特别地, 当 $P_1\neq P_2$ 时,

$$x(P_1+P_2)=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+a_1\left(\frac{y_2-y_1}{x_2-x_1}\right)-a_2-x_1-x_2,$$

当 $P_1=P_2$ 时,

$$x(2P_1)=\frac{x_1^4-b_4x_1^2-2b_6x_1-b_8}{4x_1^3+b_2x_1^2+b_4x_1+b_6},$$

其中 b_2, b_4, b_6, b_8 定义如前.

在实际应用中, 经常遇到以下两个特殊情况下的运算规则.

当 $\mathrm{char}(K) \neq 2, 3$ 时, 在方程 (7.4) 定义的 E 上, $-P = (x, -y)$. 当 $P_1 + P_2 \neq \mathcal{O}$ 时, 令

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2, \\ \dfrac{3x_1^2 + a}{2y_1}, & x_1 = x_2 \end{cases}$$

(当 $x_1 = x_2$ 时, 一定有 $y_1 \neq 0$; 否则 $P_1 = P_2 = -P_1$, 从而 $P_1 + P_2 = \mathcal{O}$), 则

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1. \end{aligned}$$

当 $\mathrm{char}(K) = 2$ 时, 在方程 (7.8) 定义的 E 上, $-P = (x, y + x)$, 当 $P_1 + P_2 \neq \mathcal{O}$ 时, 令

$$\lambda = \begin{cases} \dfrac{y_2 + y_1}{x_2 + x_1}, & x_1 \neq x_2, \\ \dfrac{x_1^2 + y_1}{x_1}, & x_1 = x_2 \end{cases}$$

(同样当 $x_1 = x_2$ 时, 一定有 $x_1 \neq 0$), 则

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + a_2 + x_1 + x_2, \\ y_3 &= (x_1 + x_3)\lambda + y_1 + x_3. \end{aligned}$$

7.1.3 同构与 j 不变量

设 E/K 为方程 (7.1) 定义的曲线, $\widehat{K}$ 为任一中间域, $K \subset \widehat{K} \subset \overline{K}$. (X, Y, Z) 为 E 上一点 $(X, Y, Z) \in \overline{K}$, 若存在 $\lambda \in \overline{K}$, 使 $(\lambda X, \lambda Y, \lambda Z) \in \widehat{K}^3 \setminus \{(0, 0, 0)\}$, 则称 (X, Y, Z) 为 $\widehat{K}$ 上的有理点, 以 $E(\widehat{K})$ 表示 E 上全体 $\widehat{K}$ 有理点的集合, 由 E 上加法的定义, 可知 $E(\widehat{K})$ 成一个子群.

在式 (7.1) 中取变换

$$\begin{aligned} \lambda : x &= u^2 x' + r, \\ y &= u^3 y' + u^2 s x' + t \end{aligned} \tag{7.11}$$

$(u, r, s, t \in \widehat{K}, u \neq 0)$, 得到同样由 Weirerstrass 方程定义的另一椭圆曲线

$$E' : y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6',$$

E 上的无穷远点变为 E' 上的无穷远点, 且

$$\begin{aligned}
ua_1' &= a_1 + 2s, \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\
u^3a_3' &= a_3 + ra_1 + 2t, \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st, \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1, \\
u^2b_2' &= b_2 + 12r, \\
u^4b_4' &= b_4 + rb_2 + br^2, \\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3, \\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4, \\
u^4c_4' &= c_4, \\
u^6c_6' &= c_6, \\
u^{12}\Delta' &= \Delta, \\
j' &= j.
\end{aligned} \tag{7.12}$$

定理 7.2 当且仅当 $\Delta \neq 0$ 时, 方程(7.1)定义的曲线 E 是非奇异的.

证明 变换 λ 建立了曲线 E 与 E' 的点之间的一一对应, 且 E 的奇点与 E' 的奇点互相对应. 对于方程 (7.4),(7.6),(7.7),(7.8) 和 (7.9) 所定义的曲线, 通过直接验算, 已经证明了当且仅当 $\Delta \neq 0$ 时为非奇异, 这些曲线都由曲线 E 通过形如 λ 的变换产生, 且已包含了所有可能的情况, 由此可见定理 7.2 成立.

λ 变换将射影平面 $\mathbb{P}^2(\widehat{K})$ 上的直线变为直线, 由椭圆曲线加法的定义, 可见 λ 保持加法不变, 即 $\lambda(P+Q) = \lambda(P) + \lambda(Q)$ $(P, Q \in E)$. 称 λ 是 $E(\widehat{K})$ 与 $E'(\widehat{K})$ 定义在 $\widehat{K}$ 上的同构 (在通常加法群意义下的同构). 式 (7.12) 表示 $\widehat{K}$ 上同构的椭圆曲线具有相同的 j 不变量 (这也就是该名称的由来). 进一步可以证明如下结论.

定理 7.3 定义在 K 上的两条椭圆曲线在 $\overline{K}$ 上同构, 当且仅当它们具有相同的 j 不变量.

证明 式 (7.12) 表明在 $\overline{K}$ 上同构的椭圆曲线具有相同的 j 不变量, 所以仅需证明具有相同 j 不变量的曲线一定在 $\overline{K}$ 上同构. 只要对方程 (7.4),(7.6),(7.7),(7.8) 和 (7.9) 定义的曲线分别证明上述结论即可. 这里仅以讨论方程 (7.4) 定义的曲线为例. 设

$$E: y^2 = x^3 + ax + b, \quad E': y^2 = x^3 + a'x + b'$$

具有相同的 j 不变量, 则由 j 的定义得

$$j = 3^3 \cdot 2^8 a^3/(4a^3 + 27b^2) = 3^3 \cdot 2^8 (a')^3/(4(a')^3 + 27(b')^2)$$

$(4a^3+27b^2\neq 0,\ 4a'^3+27b'^2\neq 0)$, 由此可得

$$a^3b'^2=a'^3b^2.$$

分别以下面三种情况, 构造 E 与 E' 的同构 $(x,y)=(u^2x',u^3y')$:

(1) $a=0$ $(j=0)$, 这时 $b\neq 0, a'=0, b'\neq 0$, 取 $u=(b/b')^{1/6}$;

(2) $b=0$ $(j=1728)$, 这时 $a\neq 0, b'=0, a'\neq 0$, 取 $u=(a/a')^{1/4}$;

(3) $ab\neq 0$ $(j\neq 0, 1728)$, 这时 $a'b'\neq 0$, 取 $u=(a/a')^{1/4}=(b/b')^{1/6}$.

7.2 除子类群

设 E/K 为椭圆曲线, E 上的点生成的形式和 (不是 7.1 节中定义的加法)

$$D=\sum_{P\in E}n_P(P).$$

称为 E 的一个除子, 这里 n_P 为整数, 对几乎所有的 $P\in E(\overline{K})$ 有 $n_P=0$. 所有除子按这种形式加法形成一个自由交换群, 称为 E 的除子群, 记为 $\mathrm{Div}(E)$. 除子 D 的次数 $\deg D$ 定义为

$$\deg D=\sum_{P\in E}n_P.$$

所有次数为零的除子组成 $\mathrm{Div}(E)$ 的一个子群, 记为 $\mathrm{Div}^{\circ}(E)$.

设 $f(x,y)=0$ $(f\in K[x,y])$ 为定义椭圆曲线 E 的方程, $f(x,y)$ 生成 $\overline{K}[x,y]$ 中一个素理想, 整环 $\overline{K}[x,y]/(f(x,y))$ 的商域称为椭圆曲线 E 的函数域, 记为 $\overline{K}(E)$(类似地, 可以定义椭圆曲线 E 在域 K 上的函数域 $K(E)$). $\overline{K}(E)$ 中的任一函数可表为 $h_1(X,Y,Z)/h_2(X,Y,Z)$, h_1 和 h_2 是次数相同的两个齐次多项式, 并且 h_2 不在 E 上恒为零.

设 $g\in\overline{K}(E)$, 定义 g 所对应的除子

$$\mathrm{div}(g)=\sum_{P\in E}\mathrm{ord}_P(g)(P),$$

这里 $\mathrm{ord}_P(g)$ 是 g 在 P 的阶 (因 P 是光滑点, $\mathrm{ord}_P(g)$ 是有定义的), 当 $\mathrm{ord}_P(g)>0$ 时, 表示 P 是 g 的 $\mathrm{ord}_P(g)$ 阶零点. 当 $\mathrm{ord}_P(g)<0$ 时, 表示 P 是 g 的 $-\mathrm{ord}_P(g)$ 阶极点. g 仅有有限个零点和极点, 对任一 $g\in\overline{K}(E)$ 都有 $\deg(\mathrm{div}(g))=0$ (参见文献 [49], 第二章命题 3.1).

函数域 $\overline{K}(E)$ 中任一函数 g 对应的除子 $\mathrm{div}(g)$ 称为主除子, 所有主除子形成 $\mathrm{Div}(E)$ 的一个子群, $\mathrm{Div}(E)$ 对它的商群称为除子类群 (或 Picard 群), 记为 $\mathrm{Pic}(E)$.

两个除子 D_1, D_2, 若存在 $g \in \overline{K}(E)$, 使

$$D_2 = D_1 + \mathrm{div}(g),$$

称 D_1 与 D_2 线性等价, 记为 $D_1 \sim D_2$, 这时有 $\deg D_1 = \deg D_2$. $\mathrm{Div}^{\circ}(E)$ 关于主除子群的商群记为 $\mathrm{Pic}^{\circ}(E)$.

记 P, Q 为 E 上两点, 通过 P 和 Q 的直线记为 $L_1 = 0$, 它与 E 交于第三点 R, 通过 R 与无穷远点 $\mathcal{O}$ 的直线 $L_2 = 0$ 与 E 交于第三点, 即为 $P + Q$, 直线 $Z = 0$ 与 E 在 $\mathcal{O}$ 点相切, 且重数为 3, 故

$$\mathrm{div}(L_1/Z) = (P) + (Q) + (R) - 3(\mathcal{O}),$$
$$\mathrm{div}(L_2/Z) = (R) + (P+Q) - 2(\mathcal{O}),$$

所以

$$\mathrm{div}(L_1/L_2) = \mathrm{div}(L_1/Z) - \mathrm{div}(L_2/Z) = (P) + (Q) - (P+Q) - (\mathcal{O}),$$

这里 $L_1/Z, L_2/Z, L_1/L_2$ 都为 $\overline{K}(E)$ 中的函数, 由此可见

$$(P) - (\mathcal{O}) + (Q) - (\mathcal{O}) \sim (P+Q) - (\mathcal{O}). \tag{7.13}$$

设 $D = \sum n_P(P)$ 为 $\mathrm{Div}^{\circ}(E)$ 中任一除子, 即 $\sum n_P = 0$, 反复利用式 (7.13) 可以发现

$$D = \sum n_P\big((P) - (\mathcal{O})\big) \sim \Big(\sum n_P P\Big) - (\mathcal{O}), \tag{7.14}$$

和式 $\sum n_P P$ 为 E 上的加法. 式 (7.14) 表示 $\mathrm{Div}^{\circ}(E)$ 中任一除子都与一形如 $(P) - (\mathcal{O})$ 的除子线性等价, 亦即映射

$$\kappa : E \longrightarrow \mathrm{Pic}^{\circ}(E)$$
$$P \longmapsto (P) - (\mathcal{O})$$

是一个群同态, 且是满射. 利用 Riemann-Roch 定理可以证明: 如果 P_1, P_2 为 E 上不同的两个点, 则 $(P_1) - (\mathcal{O})$ 与 $(P_2) - (\mathcal{O})$ 不能线性等价 (参见文献 [49], 第三章命题 3.4), 亦即 κ 是一个同构, 于是有如下定理.

定理 7.4 椭圆曲线 E 与 $\mathrm{Pic}^{\circ}(E)$ 有同构映射

$$\kappa : E \longrightarrow \mathrm{Pic}^{\circ}(E),$$
$$P \longmapsto (P) - (\mathcal{O}).$$

若 $D = \sum n_P(P) \in \mathrm{Pic}^{\circ}(E)$, 则 $\kappa^{-1}(D) = \sum n_P P$(为 E 上求和).

推论 7.1 除子 $D = \sum n_P(P)$ 为主除子的充要条件为

$$\sum n_P = 0 \quad 及 \quad \sum n_P P = \mathcal{O}.$$

7.3 同种映射

设 E_1/K 和 E_2/K 为两条椭圆曲线, ϕ 为从 E_1 到 E_2 的有理映射:

$$\begin{aligned}\phi : E_1 &\longrightarrow E_2\\(X,Y,Z) &\longmapsto (f_1(X,Y,Z), f_2(X,Y,Z), f_3(X,Y,Z)),\end{aligned}$$

其中 $f_1, f_2, f_3 \in \overline{K}(E_1)$. E_1 为非奇异曲线, 对任一 $P \in E_1$, 一定存在 $g \in \overline{K}(E_1)$, 使 gf_i $(i = 1, 2, 3)$ 在 P 点都有意义, 这时 $(gf_1(P), gf_2(P), gf_3(P)) \in E_2$, 即 ϕ 在 E_1 的任一点都有意义. 当 ϕ 不是常值映射时, ϕ 一定是映上的 (参见文献 [20], 第二章定理 6.8).

ϕ 诱导出从 $\overline{K}(E_2)$ 到 $\overline{K}(E_1)$ 的一个同态映射:

$$\begin{aligned}\phi^* : \overline{K}(E_2) &\longrightarrow \overline{K}(E_1)\\f &\longmapsto f \cdot \phi.\end{aligned}$$

当 ϕ 不是常值映射时, $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的有限扩张, 定义 ϕ 的次数为

$$\deg \phi = [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))].$$

当 ϕ 为常值映射时, 令 $\deg \phi = 0$. 当 $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的可分、不可分、纯不可分扩张时, ϕ 也相应地称为可分、不可分、纯不可分.

反之, 如果 $\tau : \overline{K}(E_2) \to \overline{K}(E_1)$ 是一个嵌入映射, 则存在有理映射 $\phi : E_1 \to E_2$, 使 $\phi^* = \tau$(参见文献 [49], 第二章定理 2.4).

ϕ 也诱导出从 $\overline{K}(E_1)$ 到 $\overline{K}(E_2)$ 的一个同态映射:

$$\begin{aligned}\phi_* : \overline{K}(E_1) &\longrightarrow \overline{K}(E_2)\\f &\longmapsto \left(\phi^*\right)^{-1} N_{\overline{K}(E_1)/\phi^*(\overline{K}(E_2))}(f),\end{aligned}$$

这里 N 是从 $\overline{K}(E_1)$ 到 $\phi^*(\overline{K}(E_2))$ 的范映射.

设 P 为 E_1 的任一点, 则存在 $t_P \in \overline{K}(E_1)$, 使 $\mathrm{ord}_P(t_P) = 1$, 函数 t_P 称为 P 的单值化子. 设 $t_{\phi(P)} \in \overline{K}(E_2)$ 为 $\phi(P)$ 的单值化子, 定义

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$$

为 ϕ 在 P 的分歧指数, 对任一 $Q \in E_2$, 有 (参考文献 [20], 第二章定理 6.9)

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi. \tag{7.15}$$

考虑 E_1 和 E_2 上的除子类群, ϕ 在 $\mathrm{Div}(E_1)$ 和 $\mathrm{Div}(E_2)$ 之间诱导两个映射 (仍记为 ϕ^* 和 ϕ_*):

$$\begin{aligned}\phi^*: \mathrm{Div}(E_2) &\longrightarrow \mathrm{Div}(E_1)\\ (Q) &\longmapsto \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P),\end{aligned}$$

以及

$$\begin{aligned}\phi_*: \mathrm{Div}(E_1) &\longrightarrow \mathrm{Div}(E_2)\\ (P) &\longmapsto (\phi(P)).\end{aligned}$$

对任一 $D\in\mathrm{Div}(E_2)$, 利用式 (7.15) 易见 $\deg(\phi^*(D)) = \deg\phi\cdot\deg D$, 所以 ϕ^* 将 $\mathrm{Div}^\circ(E_2)$ 映入 $\mathrm{Div}^\circ(E_1)$. 显然, ϕ_* 也将 $\mathrm{Div}^\circ(E_1)$ 映入 $\mathrm{Div}^\circ(E_2)$. 易见 $\phi^*\mathrm{div}(f) = \mathrm{div}(\phi^* f)\quad (f\in\overline{K}(E_2))$, 即 ϕ^* 将主除子映为主除子. 同样 ϕ_* 也将主除子映为主除子 (参见文献 [49], 第二章命题 3.6). 所以 ϕ^* 和 ϕ_* 分别诱导同态映射

$$\phi^*: \mathrm{Pic}^\circ(E_2)\longrightarrow \mathrm{Pic}^\circ(E_1)$$

和

$$\phi_*: \mathrm{Pic}^\circ(E_1)\longrightarrow \mathrm{Pic}^\circ(E_2).$$

设 ϕ 为 E_1 到 E_2 的有理映射, 若 $\phi(\mathcal{O})=\mathcal{O}$, 则称 ϕ 为同种映射.

定理 7.5 设$\phi{:}E_1\to E_2$ 为同种映射, 则是同态映射, 即对所有 $P,Q\in E_1$, 有

$$\phi(P+Q)=\phi(P)+\phi(Q).$$

证明 有群同构 (定理 7.4)

$$\begin{aligned}\kappa_i: E_i &\longrightarrow \mathrm{Pic}^\circ(E_i)\\ P &\longmapsto (P)-(\mathcal{O})\end{aligned}$$

$(i=1,2)$. 由于 $\phi(\mathcal{O})=\mathcal{O}$, 下列图是可交换的:

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \mathrm{Pic}^\circ(E_1)\\ {\scriptstyle\phi}\big\downarrow & & \big\downarrow{\scriptstyle\phi_*}\\ E_2 & \xrightarrow{\kappa_2} & \mathrm{Pic}^\circ(E_2).\end{array}$$

因 κ_1,κ_2 是同构映射, ϕ_* 是同态映射, 故 ϕ 也是同态映射.

将 E_1 到 E_2 所有的同种映射形成的加法群记为 $\mathrm{Hom}(E_1,E_2)$. 当 $E_1=E_2$ 时, 记 $\mathrm{End}(E)=\mathrm{Hom}(E,E)$. 若 $\phi,\psi\in\mathrm{End}(E)$, 将 $\phi\psi$ 理解为 ϕ 与 ψ 的复合映射, 于

是 End(E) 成为一个环, 称为 E 的自同态环. 任一整数 m, 对应 End(E) 中一个同种映射: $P \mapsto mP$, 将它表示为 $[m]$. 易见对任一 $\phi \in \mathrm{End}(E)$, 有 $\phi \cdot [m] = [m] \cdot \phi$.

设 $\phi \in \mathrm{Hom}(E_1, E_2)$, ϕ 为群同态, 故 $\mathrm{Ker}\phi = \phi^{-1}(\mathcal{O})$, 且对任一 $Q \in E_2$ 都有

$$\#\phi^{-1}(Q) = \#\phi^{-1}(\mathcal{O}) = \#\mathrm{Ker}\phi.$$

由式 (7.15), 可知 $\#\mathrm{Ker}\phi \leqslant \deg \phi$. 进一步可以证明如下定理.

定理 7.6 设 $\phi \in \mathrm{Hom}(E_1, E_2)$, 则 $\#\mathrm{Ker}\phi = \deg_s \phi$, 且对任一 $P \in E_1$ 有 $e_\phi(P) = \deg_i \phi$, 这里 $\deg_s \phi$ 和 $\deg_i \phi$ 分别表示扩张 $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ 的可分次数和不可分次数.

证明 见文献 [49], 第三章定理 4.10.

设 $\phi \in \mathrm{Hom}(E_1, E_2)$, $T \in \mathrm{Ker}\phi$, 定义 E_1 上的有理变换

$$\tau_T(P) = T + P, \quad \forall P \in E_1,$$

τ_T 诱导 $\overline{K}(E_1)$ 一个同构

$$\tau_T^*(f)(P) = f(T + P), \quad \forall f \in \overline{K}(E_1).$$

当 $f = g \cdot \phi \ \ (g \in \overline{K}(E_2))$ 时,

$$\tau_T^*(f)(P) = g(\phi(T + P)) = g(\phi(P)) = f(P),$$

即 $\phi^*(\overline{K}(E_2))$ 包含在 τ_T^* 的固定子域内.

定理 7.7 设 $\phi \in \mathrm{Hom}(E_1, E_2)$, 映射

$$\begin{aligned} \mathrm{Ker}\phi &\longrightarrow \mathrm{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))] \\ T &\longmapsto \tau_T^* \end{aligned}$$

是一个同构, 当 ϕ 可分时, $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ 是 Galois 扩张, 其 Galois 群与 $\mathrm{Ker}\phi$ 同构.

证明 若 $T, S \in \mathrm{Ker}\phi$, 易见 $\tau^*_{(S+T)} = \tau_T^* \cdot \tau_S^*$, 由定理 7.6, 有 $\#\mathrm{Ker}\phi = \deg_s \phi$, 由 Galois 理论有 $\#\mathrm{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))] \leqslant \deg_s \ \phi$, 所以仅需证明映射 $T \mapsto \tau_T^*$ 是一个单射. 假设 τ_T^* 是一个恒等变换, 则对任一 $f \in \overline{K}(E_1)$, 都有 $f(\mathcal{O}) = f(T)$, 显然这时有 $T = \mathcal{O}$. 当 ϕ 可分时有 $\#\mathrm{Ker}\,\phi = \deg\ \phi$, 即 $\#\mathrm{Aut}[\overline{K}(E_1)/\phi^*\overline{K}(E_2))] = \deg\phi$, 定理得证.

对任一 $\phi \in \mathrm{Hom}(E_1, E_2)$, 存在一个从 E_2 到 E_1 的映射

$$E_2 \xrightarrow{\kappa_2} \mathrm{Pic}^\circ(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^\circ(E_1) \xrightarrow{\kappa_1^{-1}} E_1,$$

它将 $Q\in E_2$ 映射为

$$
\begin{aligned}
\kappa_1^{-1}\phi^*\kappa_2(Q) &= \kappa_1^{-1}\phi^*\big((Q)-(\mathcal{O})\big)\\
&= \kappa_1^{-1}\left(\sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P)-\sum_{T\in\phi^{-1}(\mathcal{O})} e_\phi(T)(T)\right)\\
&= \sum_{P\in\phi^{-1}(Q)}[e_\phi(P)]P-\sum_{T\in\phi^{-1}(\mathcal{O})}[e_\phi(T)]T\\
&= [\deg_i\phi]\left(\sum_{T\in\phi^{-1}(\mathcal{O})}(P+T)-\sum_{T\in\phi^{-1}(\mathcal{O})}T\right)\\
&= [\deg_i\phi]\cdot[\deg_s\phi]\cdot P=[\deg\phi]P,
\end{aligned}
\tag{7.16}
$$

其中 P 可为 $\phi^{-1}(Q)$ 中任一点, 这里利用了定理 7.6. 可以证明上述映射是同种映射 (参见文献 [49], 第三章定理 6.1), 称它为 ϕ 的对偶, 记为 $\widehat{\phi}$, 由式 (7.16) 可知

$$
\widehat{\phi}\phi=[\deg\phi]. \tag{7.17}
$$

ϕ 的对偶 $\widehat{\phi}$ 是唯一确定的. 若有 $\widehat{\phi}'\cdot\phi=[\deg\phi]$, 则 $(\widehat{\phi}-\widehat{\phi}')\cdot\phi=[0]$, 是一个常值映射, 可见 $\widehat{\phi}-\widehat{\phi}'$ 是常值映射, 即 $\widehat{\phi}=\widehat{\phi}'$.

现在来讨论两类重要的, 一类为上述已定义的 $[m]$, 其中 m 可为任何整数, 另一类为下面即将定义的 Frobenius 变换 (当 $\mathrm{char}(K)>0$ 时).

定理 7.8 对任一整数 m, 有 $\widehat{[m]}=[m]$ 及 $\deg[m]=m^2$. 所以当 $\mathrm{char}(K)=0$ 或 $\mathrm{char}(K)$ 与 m 互素时, $[m]$ 是可分的.

证明 设 $\phi,\psi\in\mathrm{Hom}(E_1,E_2)$, 则 $\widehat{\phi+\psi}=\widehat{\phi}+\widehat{\psi}$(参见文献 [49], 第三章定理 6.2). 当 $m=0$ 或 ±1 时, 定理显然成立. 由于

$$
\widehat{[m\pm1]}=\widehat{[m]}\pm\widehat{[1]},
$$

利用归纳法, 可知第一个结论成立. 令 $d=\deg[m]$, 由式 (7.17),

$$
[d]=\widehat{[m]}\cdot[m]=[m^2],
$$

因而, $[d-m^2]=0$, 所以 $d=m^2$.

定理 7.9 设 $\phi\in\mathrm{Hom}(E_1,E_2)$, $\psi\in\mathrm{Hom}(E_2,E_3)$, 则

(1) $\deg\phi=\deg\widehat{\phi}$;

(2) $\phi\widehat{\phi}=[\deg\phi]$;

(3) $\widehat{\widehat{\phi}}=\phi$;

(4) $\widehat{\psi\phi}=\widehat{\phi}\widehat{\psi}$.

证明　(1) 记 $d=\deg\phi$, 由定理 7.8, $d^2=\deg[d]=\deg(\widehat{\phi}\phi)=\deg\widehat{\phi}\cdot\deg\phi=d\cdot\deg\widehat{\phi}$, 故 $\deg\widehat{\phi}=d$.

(2)$(\phi\widehat{\phi})\phi=\phi(\widehat{\phi}\phi)=\phi\cdot[d]=[d]\cdot\phi$, 故 $\phi\widehat{\phi}=[d]$.

(3)$[d]\widehat{\widehat{\phi}}=(\phi\widehat{\phi})\widehat{\widehat{\phi}}=\phi(\widehat{\phi}\widehat{\widehat{\phi}})=\phi[\deg\widehat{\phi}]=[d]\phi$, 故 $\widehat{\widehat{\phi}}=\phi$.

(4)$\psi\phi\cdot\widehat{\phi}\widehat{\psi}=[\deg\phi]\cdot\psi\widehat{\psi}=[\deg\phi\cdot\deg\psi]=[\deg\phi\psi]=\psi\phi\cdot\widehat{\psi\phi}$, 故 $\widehat{\psi\phi}=\widehat{\phi}\widehat{\psi}$, 证毕.

设 $\mathrm{char}(K)=p>0$, 且 $q=p^r$, E/K 为方程 (7.1) 定义的曲线, 以 $E^{(q)}$ 表示由方程

$$Y^2Z+a_1^qXYZ+a_3^qYZ^2=X^3+a_2^qX^2Z+a_4^qXZ^2+a_6^qZ^3$$

定义的曲线, 则映射

$$\phi_q:(x,y,z)\longmapsto(x^q,y^q,z^q)$$

将 E 映为 $E^{(q)}$, 且 $\phi_q(\mathcal{O})=\mathcal{O}$, 所以 $\phi_q\in\mathrm{Hom}(E,E^{(q)})$, 称为 Frobenius 变换.

设 $h(X,Y,Z)/g(X,Y,Z)\in\overline{K}(E^{(q)})$, 其中 h,g 为次数相同的齐次多项式, 则

$$\phi_q^*(h/g)=h(X^q,Y^q,Z^q)/g(X^q,Y^q,Z^q)=(h'(X,Y,Z)/g'(X,Y,Z))^q,$$

h' 和 g' 为分别将 h 和 g 的系数开 q 次方得到, 可见, $\phi_q^*(\overline{K}(E^{(q)}))=\left(\overline{K}(E)\right)^q$, $\overline{K}(E)/\phi_q^*(\overline{K}(E^{(q)}))$ 是纯不可分扩张, 即 ϕ_q 是纯不可分的, 进一步有如下定理.

定理 7.10　ϕ_q 是纯不可分的, 且 $\deg\phi_q=q$.

证明　后一结论参见文献 [49], 第二章命题 2.11.

定理 7.11　设 E_1,E_2,E_3 为定义在 K 上的椭圆曲线, $\phi\colon E_1\to E_2,\psi\colon E_1\to E_3$ 为非常值的同种映射, ϕ 可分. 若 $\mathrm{Ker}\phi\subset\mathrm{Ker}\psi$, 则存在唯一的同种映射 $\lambda\colon E_2\to E_3$, 使 $\psi=\lambda\circ\phi$.

证明　ϕ 可分, 故 $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的 Galois 扩张 (定理 7.7). 由于 $\mathrm{Ker}\phi\subset\mathrm{Ker}\psi$, 所以 $\psi^*(\overline{K}(E_3))$ 是 $\mathrm{Gal}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))$ 的一个固定子域, 且有

$$\psi^*(\overline{K}(E_3))\subset\phi^*(\overline{K}(E_2))\subset\overline{K}(E_1).$$

可见 $\psi=\lambda\cdot\phi$. 由于

$$\lambda(\mathcal{O})=\lambda(\phi(\mathcal{O}))=\psi(\mathcal{O})=\mathcal{O},$$

所以 λ 是同种映射. λ 的唯一性是显然的, 证毕.

注　若 ϕ, ψ 都定义在 K 上, 且 $\mathrm{Ker}\phi$ 中每个点都定义在 K 上, 则在定理 7.11 证明中的 $\overline{K}$ 可改换为 K, 这时亦可推出 λ 也是定义在 K 上.

7.4　Tate 模和 Weil 对

设 E/K 为椭圆曲线, m 为正整数, 定义

$$E[m] = \{P \in E(\overline{K}) \big| [m]P = \mathcal{O}\},$$

即 $E[m] = \mathrm{Ker}[m]$.

定理 7.12　(1)若 $\mathrm{char}(K) = 0$ 或 $m \geqslant 2$ 与 $\mathrm{char}(K)$ 互素, 则

$$E[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z});$$

(2) 当 $\mathrm{char}(K) = p > 0$ 时, 则

$$E[p^e] = \{\mathcal{O}\}, \quad e = 1, 2, 3, \cdots,$$

或

$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}, \quad e = 1, 2, 3, \cdots.$$

证明　当 $\mathrm{char}(K)=0$ 或 $m\geqslant 2$与$\mathrm{char}(K)$ 互素时, $[m]$ 是可分的(定理 7.8), 从而 $\#E[m] = \deg[m] = m^2$(定理 7.6). 对 m 的任一因子 d, 也可类似得到 $\#E[d] = d^2$. 利用 Abel 群的基本定理, 将 $E[m]$ 表为循环群的直积时, 仅可能有

$$E[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

当 $\mathrm{char}(K) = p > 0$ 时, 以 ϕ_p 表示 Frobenius 变换, 它是纯不可分的 (定理 7.10), 则有

$$\#E[p^e] = \deg_s[p^e] = \deg_s^e\left(\widehat{\phi_p}\phi_p\right) = \left(\deg_s \widehat{\phi_p}\right)^e,$$

因 $\deg \widehat{\phi_p} = \deg \phi_p = p$(定理 7.9), 故 $\deg_s \widehat{\phi_p} = 1$ 或 p.

当 $\deg_s \widehat{\phi_p} = 1$ 时, 对所有的 e 有 $\#E[p^e] = 1$. 当 $\deg_s \widehat{\phi_p} = p$ 时, 对所有的 e 有 $\#E[p^e] = p^e$, 从而 $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$, 证毕.

设 l 为素数, 相对于映射

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

的反向极限群

$$T_l(E) = \varprojlim_n E[l^n]$$

称为 E 的 (l-adic)Tate 模. $T_l(E)$ 中任一元素可表为

$$\alpha = (\alpha_1, \alpha_2, \cdots,),$$

其中 $\alpha_i \in E[l^i]$, 且 $[l]\alpha_{i+1} = \alpha_i (i = 1, 2, \cdots)$. 因 $E[l^i]$ 是 $\mathbb{Z}/l^i\mathbb{Z}$ 上的模, 故 $T_l(E)$ 是

l-adic 整数环 $\mathbb{Z}_l$ 上的模. 取 $u = \sum_{i=0}^{\infty} a_i l^i \in \mathbb{Z}_l$, 则

$$u \cdot \alpha = (u\alpha_1, u\alpha_2, \cdots) = (a_0\alpha_1, (a_0 + a_1 l)\alpha_2, \cdots) \in T_l(E).$$

由定理 7.12 可知, 当 $l \neq \text{char}(K)$ 时, $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$; 当 $l = \text{char}(K)$ 时, $T_l(E) \cong \{0\}$ 或 $\mathbb{Z}_l$.

设 $\text{char}(K) = 0$ 或 $m \geqslant 2$ 且与 $\text{char}(K)$ 互素, $T \in E[m]$, 则存在 $f \in \overline{K}(E)$, 使

$$\text{div}(f) = m(T) - m(\mathcal{O})$$

(推论 7.1), 取 $T' \in E(\overline{K})$, 使 $[m](T') = T$. 同样存在 $g \in \overline{K}(E)$, 使

$$\text{div}(g) = [m]^*(T) - [m]^*(\mathcal{O}) = \sum_{R \in E[m]} (T' + R) - (R),$$

易见, $f \cdot [m]$ 与 g^m 具有相同的除子, 它们仅差 $\overline{K}^*$ 中一个常数因子, 可以假设

$$f \cdot [m] = g^m.$$

设 $S \in E[m]$ (S 与 T 可以相同), 对任一 $X \in E$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m,$$

故

$$e_m(S, T) = g(X + S)/g(X)$$

是一个 m 次单位根 ($\overline{K}(E)$ 中的任一函数或常数, 或取遍 $\overline{K} \cup \{\infty\}$ 所有的值, 所以 $e_m(S, T)$ 是一个常数). g 的取法可以差一个常数因子, 但这不影响 $e_m(S, T)$ 的值. 故得到

$$e_m : E[m] \times E[m] \longrightarrow \mu_m,$$

μ_m 为 m 次单位根组成的群, e_m 称为 Weil 对.

Weil 对还有一个等价的定义, 它更便于计算. 设 $S, T \in E[m]$, 取除子 D_S 和 D_T, 使 $D_S \sim (S) - (\mathcal{O}), D_T \sim (T) - (\mathcal{O})$, 且 D_S 与 D_T 的表达式中不出现公共的支撑 (例如, 取 $D_S = ([k+1]S) - ([k]S)$, 使 $[k+1]S, [k]S, T, \mathcal{O}$ 互不相同), 存在 $f_S, f_T \in \overline{K}(E)$, 使 $\text{div}(f_S) = mD_S, \text{div}(f_T) = mD_T$. 若 $f \in \overline{K}(E), \text{div}(f)$ 与除子 $D = \sum n_P(P)$ 没有公共支撑, 则定义 $f(D) = \prod f(P)^{n_P}$. 所以有

$$e_m(S, T) = f_S(D_T)/f_T(D_S). \tag{7.18}$$

上式证明见文献 [49], 第三章习题 3.16.

定理 7.13 Weil对具有下述性质(设 $S,S_1,S_2,T,T_1,T_2\in E[m]$):

(1) 双线性:

$$e_m(S_1+S_2,T)=e_m(S_1,T)e_m(S_2,T),$$
$$e_m(S,T_1+T_2)=e_m(S,T_1)e_m(S,T_2);$$

(2) 交错性:

$$e_m(S,T)=e_m(T,S)^{-1};$$

(3) 非退化: 若对任一 $S\in E[m]$, 有 $e_m(S,T)=1$, 则 $T=\mathcal{O}$;

(4) 对任一 $\delta\in G_{\overline{K}/K}$, 有 $e_m(S,T)^\delta=e_m(S^\delta,T^\delta)$;

(5) 若 $S\in E[mm']$, $T\in E[m]$, 则 $e_{mm'}(S,T)=e_m([m']S,T)$.

证明 (1) 因

$$\begin{aligned}e_m(S_1+S_2,T)=&\frac{g(X+S_1+S_2)}{g(X)}=\frac{g(X+S_1+S_2)}{g(X+S_1)}\cdot\frac{g(X+S_1)}{g(X)}\\=&e_m(S_2,T)e_m(S_1,T),\end{aligned}$$

第一式成立. 假设对 T_1,T_2,T_1+T_2 如上述分别构造了函数 f_1,f_2,f_3,g_1,g_2,g_3, 取 $h\in\overline{K}(E)$, 使

$$\operatorname{div}(h)=(T_1+T_2)-(T_1)-(T_2)+(\mathcal{O}),$$

则 $\operatorname{div}(f_3/f_1f_2)=m\operatorname{div}(h)$, 即 $f_3=cf_1f_2h$, c 为 $\overline{K}^*$ 中一常数. 利用 $f_i\cdot[m]=g_i^m$, 并开 m 次方得 $g_3=c'g_1g_2(h\cdot[m])$, c' 为一常数, 从而

$$\begin{aligned}e_m(S,T_1+T_2)&=\frac{g_3(X+S)}{g_3(X)}=\frac{g_1(X+S)g_2(X+S)h([m]X+[m]S)}{g_1(X)g_2(X)h([m]X)}\\&=e_m(S,T_1)\ e_m(S,T_2).\end{aligned}$$

(2) 由 (1)

$$e_m(S+T,S+T)=e_m(T,T)e_m(T,S)e_m(S,T)e_m(S,S),$$

仅需要证明对任一 $T\in E[m]$ 有 $e_m(T,T)=1$. 以 τ_T 表示平移变换 $P\mapsto P+T$, 如上述构造 f 与 g, 由于

$$\operatorname{div}\left(\prod_{i=0}^{m-1}f\circ\tau_{[i]T}\right)=m\left\{\sum_{i=0}^{m-1}([1-i]T)-\sum_{i=0}^{m-1}([-i]T)\right\}=0,$$

故 $\prod\limits_{i=0}^{m-1}f\circ\tau_{[i]T}$ 是一个常数. 取 T' 使 $[m]T'=T$, 由于

$$g(X+[i]T')^m=f([m]X+[mi]T')=f([m]X+[i]T),$$

故 $\prod_{i=0}^{m-1} g\circ\tau_{[i]T'}$ 也是常数, 它在 X 与 $X+T'$ 上取相同的值, 即

$$\prod_{i=0}^{m-1} g(X+[i]T') = \prod_{i=0}^{m-1} g(X+[1+i]T'),$$

由此推出 $g(X)=g(X+T)$. 所以

$$e_m(T,T)=\frac{g(X+T)}{g(X)}=1.$$

(3) 若对所有的 $S\in E[m]$ 有 $e_m(S,T)=1$, 则对所有的 $S\in E[m]$ 有 $g(X+S)=g(X)$, 即 g 在 τ_S^* 作用下不变. $[m]$ 是可分的, 所以 $\mathrm{Gal}(\overline{K}(E)/[m]^*\overline{K}(E))\cong\{\tau_S^*|S\in E[m]\}$(定理 7.7), 因而 $g\in[m]^*\overline{K}(E)$, 存在 $h\in\overline{K}(E)$, 使 $g=h\cdot[m]$. 由于 $(h\cdot[m])^m=g^m=f\cdot[m]$, 可知 $f=ch^m$ $(c\in\overline{K}^*)$, 从而

$$m\mathrm{div}(h)=\mathrm{div}(f)=m(T)-m(\mathcal{O}),$$

可见 $\mathrm{div}(h)=(T)-(\mathcal{O})$, 左端为主除子, 故 $T=\mathcal{O}$(推论 7.1).

(4) 设 $\delta\in G_{\overline{K}/K}$, f, g 为上述对应 T 构造的函数, 则对应 T^δ 构造的函数为 f^δ, g^δ (f^δ 表示将 δ 作用到有理函数 f 的所有系数上所得到的函数), 有

$$e_m(S^\delta,T^\delta)=\frac{g^\delta(X+S^\delta)}{g^\delta(X)}=\Big(\frac{g(X+S)}{g(X)}\Big)^\delta=e_m(S,T)^\delta.$$

(5) 有

$$\mathrm{div}(f^{m'})=m'm(T)-m'm(\mathcal{O})$$

及

$$(g\circ[m'])^{mm'}=(f\circ[mm'])^{m'}=f^{m'}\circ[mm'],$$

故

$$e_{mm'}(S,T)=\frac{g\circ[m'](X+S)}{g\circ[m'](X)}=\frac{g([m']X+[m']S)}{g([m']X)}=e_m([m']S,T).$$

定理 7.14　*存在* $S,T\in E[m]$, *使* $e_m(S,T)$ *为* m *次本原单位根. 特别地, 当* $E[m]\subset E(K)$ *时, 有* $\mu_m\subset K$.

证明　若存在 m 的真因子 d 使 $e_m(S,T)^d=1$ $(\forall S,T\in E[m])$, 由于 $e_m(S,T)^d=e_m([d]S,T)=1$ 对所有的 $T\in E[m]$ 成立, 所以 $[d]S=\mathcal{O}$(定理 7.13 (3)), S 为 $E[m]$ 中任一点, 这不可能.

当 $E[m]\subset E(K)$ 时, $e_m(S,T)$ 在 $G_{\overline{K}/K}$ 作用下固定不变 (定理 7.13 (4)), 故 $e_m(S,T)\in K$, 即 $\mu_m\subset K$, 证毕.

定理 7.15 设 $\phi \in \mathrm{Hom}(E_1, E_2)$, $S \in E_1[m], T \in E_2[m]$, 则

$$e_m(\phi(S), T) = e_m(S, \widehat{\phi}(T)).$$

证明 对于 T, 如上构造函数 f 和 g, 由于 $\kappa_1(\widehat{\phi}(T)) = \phi^*((T)) - \phi^*((\mathcal{O}))$, 即 $\widehat{\phi}(T)$ 是除子 $\phi^*((T)) - \phi^*((\mathcal{O}))$ 中出现的所有点 (在 E_1 上) 之和. 利用推论 7.1, 存在 $h \in \overline{K}(E_1)$ 使

$$\phi^*((T)) - \phi^*((\mathcal{O})) = \left(\widehat{\phi}(T)\right) - (\mathcal{O}) + \mathrm{div}(h).$$

上式左端乘 m 即为 $\mathrm{div}(f \circ \phi)$(参见文献 [49], 第二章命题 3.6). 故

$$\mathrm{div}\left(\frac{f \circ \phi}{h^m}\right) = m(\widehat{\phi}(T)) - m(\mathcal{O}),$$

而

$$\frac{f \circ \phi}{h^m} \circ [m] = \frac{f \circ [m] \circ \phi}{h^m \circ [m]} = \left(\frac{g \circ \phi}{h \circ [m]}\right)^m,$$

因此

$$\begin{aligned} e_m(S, \widehat{\phi}(T)) &= \frac{(g \circ \phi / h \circ [m])(X + S)}{(g \circ \phi / h \circ [m])(X)} \\ &= \frac{g(\phi(X) + \phi(S)) h([m]X)}{g(\phi(X)) \cdot h([m]X + [m]S)} = e_m(\phi(S), T). \end{aligned}$$

设 l 为异于 $\mathrm{char}(K)$ 的素数, 将 $E[l^n]$ $(n = 1, 2, \cdots)$ 上的 Weil 对合并在一起可以得到 Tate 模 $T_l(E)$ 上的 (l-adic)Weil 对. 对应 l 次升幂映射

$$\mu_{l^{n+1}} \xrightarrow{\ l\ } \mu_{l^n}$$

定义反向极限群

$$T_l(\mu) = \varprojlim_n \mu_{l^n}.$$

设 $a = \sum_{i=0}^{\infty} a_i l^i \in \mathbb{Z}_l$, $\Lambda = (\lambda_1, \lambda_2, \cdots) \in T_l(\mu)$, 定义

$$a\Lambda = (\lambda_1^a, \lambda_2^a, \cdots) = (\lambda_1^{a_0}, \lambda_2^{a_0 + a_1 l}, \cdots),$$

$T_l(\mu)$ 可看成 $\mathbb{Z}_l$ 上的模.

设 $S = (S_1, S_2, \cdots) \in T_l(E)$, $T = (T_1, T_2, \cdots) \in T_l(E)$, 其中 S_n 和 T_n 属于 $E[l^n]$. 令

$$e(S, T) = (e_l(S_1, T_1), e_{l^2}(S_2, T_2), \cdots),$$

由于

$$e_{l^{n+1}}(S_{n+1}, T_{n+1})^l = e_{l^{n+1}}(S_{n+1}, [l]T_{n+1}) = e_{l^n}([l]S_{n+1}, T_n) = e_{l^n}(S_n, T_n)$$

(定理 7.13 的 (1) 和 (5)), 可见 $e(S,T)\in T_l(\mu)$, 从而得到 Tate 模上的 Weil 对

$$e: T_l(E)\times T_l(E)\longrightarrow T_l(\mu),$$

由定理 7.13, 易证 e 也具有双线性、交错性、非退化性. 同样地, 若 $\phi\in \mathrm{Hom}(E_1,E_2)$, $S\in T_l(E_1)$, $T\in T_l(E_2)$, 则

$$e(\phi(S),T)=e(S,\widehat{\phi}(T)),$$

这里 $\phi(S)=(\phi(S_1),\ \phi(S_2),\cdots)$.

7.5 有限域上的椭圆曲线

设 $K=F_q$(包含 q 个元素的有限域), E/K 为定义在有限域上的椭圆曲线. 令

$$E(K)=\{(x,y)\in E|x,y\in K\}\cup\{\mathcal{O}\},$$

$E(K)$ 称为 E 的 K-有理点集合, 它是一个有限集. 计算 $\#E(K)$ 是研究定义在有限域上的椭圆曲线的一个核心问题.

在方程 (7.2) 中, 当 x 取遍 F_q 的元素时, 约有一半的情况使式 (7.2) 左端的二次方程有两个解, 所以 $\#E(K)$ 大致为 $q+1$. Artin 在他的博士论文中猜想有下述定理 7.16, 后来 Hasse 给出了证明.

定理 7.16 设 $K\in F_q$, E/K 为椭圆曲线, 则

$$|\#E(K)-q-1|\leqslant 2\sqrt{q}.$$

证明 在 $E(\overline{K})$ 上定义 q 阶 Frobenius 变换

$$\begin{aligned}\phi: E&\longrightarrow E\\(x,y)&\longmapsto (x^q,y^q),\end{aligned}$$

且 $\phi(\mathcal{O})=\mathcal{O}$. 当且仅当 $\phi(P)=P$ 时, $P\in E(K)$, 所以 $E(K)=\mathrm{Ker}(1-\phi)$. 由于 $1-\phi$ 是可分的 (参见文献 [49], 第三章推论 5.5), 因而 $\#E(K)=\deg(1-\phi)$, 利用下述引理 7.2 可证得本定理.

设 A 为交换群, 函数

$$d: A\longrightarrow \mathbb{R}\ (\text{实数域})$$

称为二次型, 如果

(1) 对任意 $\alpha\in A$, $d(-\alpha)=d(\alpha)$;

(2) 令

$$\begin{aligned}A\times A&\longrightarrow \mathbb{R}\\(\alpha,\beta)&\longmapsto d(\alpha+\beta)-d(\alpha)-d(\beta),\end{aligned}$$

(α, β) 具有双线性.

一个二次型称为正定的, 如果

(3) 对任一 $\alpha \in A$, $d(\alpha) \geqslant 0$;

(4) 当且仅当 $\alpha = 0$ 时, $d(\alpha) = 0$.

引理 7.1 设 E_1, E_2 为定义在同一域上的椭圆曲线, 则映射

$$\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

是正定二次型.

证明 仅需证明若 $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, 则

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi$$

具有双线性, 其他条件显然符合. 利用式 (7.17), 有

$$\begin{aligned}[\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ &= (\widehat{\phi + \psi})(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi = \widehat{\phi}\psi + \widehat{\psi}\phi.\end{aligned}$$

易见双线性成立.

引理 7.2 设 A 为交换群, $d : A \longrightarrow \mathbb{Z}$ 为正定二次型, 则对所有 ϕ, $\psi \in A$ 有

$$|d(\phi - \psi) - d(\phi) - d(\psi)| \leqslant 2\sqrt{d(\phi)d(\psi)}.$$

证明 令 $L(\phi, \psi) = d(\phi - \psi) - d(\phi) - d(\psi)$, L 具有双线性, 利用归纳法易证 $d(m\phi) = m^2 d(\phi)$. 任取 $m, n \in \mathbb{Z}$,

$$mnL(\phi, \psi) = L(m\phi, n\psi) = d(m\phi - n\psi) - m^2 d(\phi) - n^2 d(\psi),$$

由于 d 是正定的, 故

$$0 \leqslant d(m\phi - n\psi) = m^2 d(\phi) + mnL(\phi, \psi) + n^2 d(\psi),$$

因而它的判别式 $L^2(\phi, \psi) \leqslant 4d(\phi)d(\psi)$, 即得引理.

在引理 7.2 中取 $A = \mathrm{End}(E)$, ϕ 为 q 阶 Frobenius 变换, $\psi = 1$, 由于 $\deg(1-\phi) = \#E(K)$, $\deg \phi = q$, $\deg \psi = 1$, 由此可证明定理 7.16.

设 $\psi \in \mathrm{End}(E)$, 素数 l 与 q 互素. ψ 与 $[l^n]$ 可交换, 所以 $\psi(E[l^n]) \subset E[l^n]$, ψ 可诱导 Tate 模 $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ 上的一个线性变换 ψ_l. 当 $T_l(E)$ 取定一组 $\mathbb{Z}_l$ 基后, ψ_l 可用 $\mathbb{Z}_l$ 上的一个二阶方阵表示, 因而相应可计算 $\det \psi_l$, $\mathrm{tr}(\psi_l)$.

定理 7.17 设 $\psi \in \mathrm{End}(E)$, 则

$$\det(\psi_l) = \deg\psi, \quad \mathrm{tr}(\psi_l) = 1 + \deg\psi - \deg(1-\psi).$$

可见, $\det(\psi_l)$ 和 $\mathrm{tr}(\psi_l)$ 都是整数, 且不依赖于 l.

证明 取 v_1, v_2 为 $T_l(E)$ 的 $\mathbb{Z}_l$ 基, 在这组基上,

$$\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z}_l.$$

设 e 为 $T_l(E)$ 上的 Weil 对, 则有

$$\begin{aligned} e(v_1, v_2)^{\deg\psi} &= e([\deg\psi]v_1, v_2) = e(\widehat{\psi}\psi v_1, v_2) \\ &= e(\psi v_1, \psi v_2) = e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det(\psi_l)}, \end{aligned}$$

这里利用了 $e(v_1, v_1) = e(v_2, v_2) = 1$, $e(v_2, v_1) = e(v_1, v_2)^{-1}$. 由于 e 是非退化的, 故得 $\det(\psi_l) = \deg\psi$. 对于任意二阶方阵 A 都有

$$\det(1 - A) = 1 + \det A - \mathrm{tr}(A).$$

于是得到 $\mathrm{tr}(\psi_l)$ 的表达式.

设 ϕ 为 q 阶 Frobenius 变换, 可见 ϕ_l 的特征多项式为

$$\det(T - \phi_l) = T^2 - \mathrm{tr}(\phi_l)T + \deg\phi_l = T^2 - tT + q,$$

其中, t 为不依赖于 l 的整数, 称为 ϕ 的迹. 由于 $\phi_l^2 - t\phi_l + q = 0$, 这表示 $\phi^2 - t\phi + q$ 在 $E[l^n]$ $(n = 1, 2, \cdots)$ 上的作用恒为 $\mathcal{O}$, 因而它在 E 上的作用恒为 $\mathcal{O}$, 即 $\phi^2 - t\phi + q = 0$, ϕ 适合二次方程 $x^2 - tx + q = 0$. 利用定理 7.17 的第两个恒等式 (取 $\psi = \phi$),

$$\#E(K) = \deg(1 - \phi) = 1 + q - t, \tag{7.19}$$

因而 $|t| \leqslant 2\sqrt{q}$(定理 7.16), 二项式 $x^2 - tx + q$ 有两个根 α, β(在复数域中), 且 $|\alpha| = |\beta| = \sqrt{q}$, α 和 β 就是 ϕ_l 的特征根, ϕ_l^n 的特征根就是 α^n 和 β^n. 记 $K_n = F_{q^n}$, ϕ^n 为 q^n 阶 Frobenius 变换, 因而

$$\begin{aligned} \#E(K_n) &= \mathrm{Ker}(1 - \phi^n) = \deg(1 - \phi^n) = \det(1 - \phi_l^n) \\ &= 1 + \det(\phi_l^n) - \mathrm{tr}(\phi_l^n) = 1 + q - \alpha^n - \beta^n. \end{aligned} \tag{7.20}$$

令 $V_0=2, V_1=t=\alpha+\beta, V_n=tV_{n-1}-qV_{n-2}\ (n\geqslant 2)$, 易见 $V_n=\alpha^n+\beta^n$. 利用这个递推公式可以方便地计算 V_n. 最初的几个 V_n 为

$$\begin{aligned}
V_2&=t^2-2q,\\
V_3&=t^3-3tq,\\
V_4&=t^4-4t^2q+2q^2,\\
V_5&=t^5-5t^3q+5tq^2,\\
V_6&=t^6-6t^4q+9t^2q^2-2q^3,\\
V_7&=t^9-7t^5q+14t^3q-7tq^3.
\end{aligned} \tag{7.21}$$

习　题

习题 7.1　令 $p\neq 2$ 是素数, $a,b,c,d\in F_p$ 满足 $acd\neq 0$, C 是满足二次方程

$$ax^2+bxy+cy^2=dz^2$$

的圆锥曲线. 证明:

(1) 若 $b^2\neq 4ac$, 则 $|C(F_p)|=p+1$;

(2) 若 $b^2=4ac$, 则要么 $|C(F_p)|=1$, 要么 $|C(F_p)|=p+1$;

(3) 给出例子说明上述三种可能性都会出现.

习题 7.2　素数 p 分别取 $3,7,11,13$, $E/F_p: y^2=x^3+x+1$, 求 $|E(F_p)|$.

习题 7.3　令素数 $p\equiv 3(\mathrm{mod}4)$, $b\in F_p^*$.

(1) 证明: 方程 $C: v^2=u^4-4b$ 在 F_p^2 中有 $p-1$ 个解.

(2) 令 $E: y^2=x^3+bx$, 那么

$$\begin{aligned}
\varphi: C(F_p)&\longrightarrow E(F_p)\\
(u\ v)&\longmapsto\left(\frac{1}{2}(u^2+v),\frac{1}{2}u(u^2+v)\right)
\end{aligned}$$

是一个映射.

(3) 证明 $|C(F_p)|=p+1$.

习题 7.4　令 $q=2^r$, $E/F_q: y^2+y=x^3$.

(1) 用点 P 的 x,y 坐标来表示 $-P$ 和 $2P$ 的坐标.

(2) 若 $q=16$, 证明 E 中的每一个非零点的阶均为3.

(3) 求 $|E(F_{2^2})|$ 和 $|E(F_{2^4})|$.

第 8 章　密码学中的一些应用

8.1　RSA 公钥密码

在使用传统密码加密信息时, 信息的发方将明文 m(它通常用一个 0-1 序列表示, 通过整数的二进制, 也可把它表示为一个整数) 通过加密运算

$$c = E_k(m)$$

变为密文 c 后发给收方. 收方接到密文 c 之后, 利用解密运算

$$m = D_k(c)$$

得到明文 m. 这里 k 是一个密钥, 它参与运算, 对同一个明文选用不同的密钥可以得到不同的密文, 这可以增加敌方破译的难度. 密钥是不能泄露的. 在传统的密码中, 加密和解密使用同样的密钥, 因此在通信前, 发方和收方必须通过一个安全信道约定所选用的密钥.

在计算机网络环境下, 用户的数量可以很多, 相互之间的业务关系也不是固定的, 利用上述传统的密码是不方便的. 在 20 世纪 70 年代, 提出了公钥密码的概念. 在这种系统中, 每个用户有两个密钥, 一个公开, 一个保密, 分别称为公钥和私钥, 并且要求从一个用户的公钥很难推算出他的私钥.

Rivest, Shamir 和 Adleman 在 1978 年发表的题为《数字签名和公钥密码的一个方法》一文中, 提出了一个公钥密码, 现在人们称它为 RSA 公钥密码.

成立一个密钥分发中心, 一个用户如要使用密码, 就去该中心登记领取密钥. 密钥分发中心选用一个正整数 $n = pq$, 这里 p 和 q 是两个不同的素数, 通常很大. n 是公开的, 而 p, q 是保密的, 我们知道 $\varphi(n) = (p-1)(q-1)$, 但是如果不知道 p 和 q, 即不知道 n 的因子分解, 就不能利用这个公式计算 $\varphi(n)$.

当一个用户来中心登记领取密钥时, 中心给他选取一个数 e, e 为小于 $\varphi(n)$ 且与它互素的正整数. 利用辗转相除法, 可以找到整数 d 和 x, 使

$$ed + x\varphi(n) = 1, \tag{8.1}$$

即

$$ed \equiv 1 \pmod{\varphi(n)},$$

e 作为用户的公钥, d 作为用户的私钥.

只要知道了该用户 A 的公钥 e 和 n, 任何人 B 都可向他发加密报文. 设明文

$$m = (m_0, m_1, \cdots, m_l), \quad m_i = 0, 1,$$

将 m 表成一个整数

$$m = m_0 + 2m_1 + \cdots + 2^l m_l,$$

今后都用这种方式将明文表为一个整数. 假设 $m < n$, 且 m 与 n 互素 (m 与 n 不互素的情况, 出现的可能性极小). 发方 B 利用 A 的公钥 e 将 m 加密成密文

$$c \equiv m^e \pmod n,$$

B 将密文 c 经由公开的通信信道给A. A 在收到 c 后利用他的私钥解密计算 $c^d \pmod n$, 由式 (8.1), 则有 $ed = 1 - x\varphi(n)$, 因此

$$c^d \equiv m^{ed} \equiv m^{1-x\varphi(n)} \equiv m \cdot \left(m^{\varphi(n)}\right)^{-x} \pmod n,$$

这里利用了定理 2.5. 这样 A 从密文 c 就得出了明文 m.

如果不知道 $\varphi(n)$, 由已知的公钥 e 很难算私钥 d, 若知道 $\varphi(n)$, 则由

$$pq = n, \quad p + q = n - \varphi(n) + 1$$

可知 p, q 是二次方程 $x^2 + (\varphi(n) - n - 1)x + n = 0$ 的根, 可以算出 p, q, 从而将 n 因子分解. 所以 RSA 公钥密码的安全性与因子分解密切相关. 若能知道 n 的因子分解, 该密码就能破了. 因此要选用足够大的 n, 使得在当今技术条件下要分解它是困难的. 自从 RSA 公钥密码问世后, 大大刺激了整数因子分解计算方法的研究. 利用很多高深的数学知识, 结合计算机的应用, 提出了不少新的因子分解的算法 (详见第 10 章).

要选用足够大的 n, 就要产生足够大的素数 p 和 q, 这里遇到的问题实际上是要求能够判断一个整数是否是素数, 它在理论上已较好地得到解决, 利用计算机产生一百多位的素数并不困难.

在选择 p 和 q 时, 也有些因素要考虑, 以便使 n 难以分解. 例如, 当 p 和 q 很接近时, n 就容易分解. 因为

$$n = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2,$$

当 $(p-q)/2$ 很小时, $t = (p+q)/2$ 很接近 $\sqrt{n}$, 因此逐个检查大于 $\sqrt{n}$ 的 t, 看它能否使 $t^2 - n$ 是一个平方数, 若有 $t^2 - n = s^2$, 则可得到 n 的因子分解

$$n = t^2 - s^2 = (t+s)(t-s),$$

所以 p 和 q 不能太接近.

除分解 n 的因子之外, 是否还有其他攻击 RSA 的方法? 今举个例子: 第三者在截获 c 后, 反复计算它的 e 次幂, 可得

$$c^e \equiv m^{e^2}, \quad c^{e^2} \equiv m^{e^3}, \cdots \pmod{n}.$$

一旦出现 $c^{e^t} \equiv c \pmod{n}$, 就有 $c^{e^{t-1}} \equiv m \pmod{n}$, 即在出现 c 之前的计算结果就是明文 m, 当 t 不很大时, 这种攻击也是可行的. $c^{e^{t-1}} \equiv m \pmod{n}$ 就是 $m^{e^t} \equiv m \pmod{n}$, 即 $n|m^{e^t-1}-1$, 若 m 模 n 的阶为 k, 则

$$e^t \equiv 1 \pmod{k},$$

t 可取的最小值就是 e 模 k 的阶, 必须使这阶尽可能大. e 模 k 的阶是 $\varphi(k)$ 的因子, 因此, 最好 $\varphi(k)$ 中有大的素因子. 又由于 k 是 m 模 n 的阶, 所以 k 是 $\varphi(n) = (p-1)(q-1)$ 的因子. 故最好使 $p-1$ 和 $q-1$ 出现大素因子. 上述讨论建议选取这样的素数 p, 使 $p-1$ 至少有一个大的素因子. 对 q 也有同样的要求.

8.2　Diffie–Hellman 体制

8.1 节提到, 在使用传统密码时, 由于加密运算和解密运算使用同样的密钥, 所以在通信前, 发方和收方必须通过一个安全通道约定所选用的密钥. 例如, 由信使预先派送在今后一段时间内所使用的密钥. 也称这类密码为对称密码. 公钥密码也称非对称密码, 它的加密运算和解密运算使用不同的密钥.

Diffie 和 Hellman[14] 提出了一个在网络环境下使用对称密码前设置密钥的新方法. 发方和收方可以通过在非安全的公共信道上的一次信息交换, 确定所使用的密钥. 任何第三方即使从公共信道上截获他们传输的信息, 也不能得到该密钥. 以 A, B 表示通信双方. 设 p 为一个大素数, g 为模 p 的原根, p 和 g 是公开的参数.

A 选取整数 $0 < a < p$, 将 $g^a \pmod{p}$ 传输给 B;

B 选取整数 $0 < b < p$, 将 $g^b \pmod{p}$ 传输给 A;

A 计算 $(g^b)^a \equiv g^{ab} \pmod{p}$, B 计算 $(g^a)^b \equiv g^{ab} \pmod{p}$, $g^{ab} \pmod{p}$ 就是 A 和 B 约定使用的密钥.

第三方可以知道 p, g 及 $g^a \pmod{p}$, $g^b \pmod{p}$, 利用这些数据, 能否得到 $g^{ab} \pmod{p}$, 这称为 Diffie-Hellman 问题. 已知 p, g 及 $n \in (\mathbb{Z}/p\mathbb{Z})^*$, 求整数 x, 使 $n \equiv g^x \pmod{p}$, 这称为模 p 的离散对数问题. 易见, 若能计算模 p 的离散对数, 就能解决 Diffie-Hellman 问题. 是否存在不计算离散对数也能解决 Diffie-Hellman 问题的方法目前尚无答案.

Diffie-Hellman 体制的安全性是基于计算离散对数问题的复杂性, 也可以用其他的群来代替 $(\mathbb{Z}/p\mathbb{Z})^*$. 例如, 任一有限域 $GF(q)$ 的乘法群或代数数域的理想类群等, 在第 11 章将介绍基于椭圆曲线离散对数的密码体制.

在网络环境下使用上述 Diffie-Hellman 体制, 也存在一些不安全的因素. 例如, 通信的一方不能知道通信另一方的身份, 有可能被人蒙骗. 因而后来在此基础上又提出了一些更复杂的体制.

8.3 ElGamal 算法

本节介绍 ElGamal 加密算法和数字签名算法.

首先介绍 ElGamal 加密算法. 在一个通信系统中, 选取一个大素数 p, 模 p 的原根 α, 一个正整数 $a\,(< p-1)$, 然后计算 $\beta \equiv \alpha^a(\bmod p)$. 将 p, α, β 公开, a 是要保密的, 不能让系统之外的人知道, 令 A 欲将信息 m 秘密发送给 B(这里假定 $0 \leqslant m < p$; 否则, 需要将 m 分为若干段, 每段小于 p. A 任选一正整数 $k\,(< p-1)$, 然后计算 $y_1 = \alpha^k(\bmod p)$, $y_2 \equiv m\beta^k(\bmod p)$, A 将 (y_1, y_2) 发送给 B. B 收到 (y_1, y_2) 后, 由于他知道 a, 于是计算

$$y_2(y_1^a)^{-1} \equiv m\beta^k \cdot \alpha^{-ak} \equiv m\,(\bmod p),$$

可以解密得到 m. 易见, 上述 ElGamal 加密算法的安全性依赖于计算模 p 的离散对数的复杂性: 即知道 α 和 β, 很难计算 a, 使 $\beta \equiv \alpha^a(\bmod p)$.

现在介绍 ElGamal 数字签名算法. A 欲将信息 m 签名后发送给 B. 仍采用上面的符号 p, m, α, a, $\beta \equiv \alpha^a(\bmod p)$, 但现在 a 仅有 A 知道. A 随机选取正整数 k $(< p-1)$, 且 k 与 $p-1$ 互素. A 计算 $\gamma \equiv \alpha^k(\bmod p)$, 并由

$$k \cdot \delta + a\gamma \equiv m\,(\bmod p-1)$$

解出 $\delta \equiv (m - a\gamma)k^{-1} \bmod (p-1)$. A 将 (m, γ, δ) 发送给 B, 这里 (γ, δ) 就是 A 对信息 m 的数字签名.

B 在收到 (m, γ, δ) 后, 检验 $\beta^\gamma \gamma^\delta \equiv \alpha^m(\bmod p)$ 是否成立, 倘若该式成立, B 认为这是 A 签名后发来的信息, 否则 B 拒收. 因为当 (m, γ, δ) 是 A 签名后发出的信息时, 一定有

$$\beta^\gamma \gamma^\delta \equiv \alpha^{a\gamma} \cdot \alpha^{k\delta} \equiv \alpha^{a\gamma} \cdot \alpha^{m-a\gamma} \equiv \alpha^m\,(\bmod p).$$

ElGamal 数字签名算法的安全性同样是依赖于离散对数问题的复杂性, 在 11.7 节中, 将讨论计算模 p 离散对数的一些方法. 在现在的技术条件下, 当 $|p| \geqslant 1024$ 比特时, 计算模 p 的离散对数是不可行的.

8.4　基于背包问题的公钥密码

有物体若干及背包一个, 由于背包太小, 不能将所有物体放入, 今问如何选择一部分物体放入, 能使背包的容积得到最充分的利用, 这就是背包问题.

将上述问题稍加演变, 给定 n 个正整数 $a_1, a_2, \cdots, a_n$ 及一个正整数 s, 已知 s 是某一些 a_i 之和, 试确定这些 a_i, 今后把这个问题称为背包问题. 从 $a_1, a_2, \cdots, a_n$ 中选出一个子集, 很容易算出这个子集之和. 但反过来, 给定一个子集的各数之和, 要确定这个子集, 一般来说就很困难了. $a_1, a_2, \cdots, a_n$ 共有 2^n-1 个非空子集, 只有将这些子集一一试过, 去找所要的子集.

利用背包问题, 可以得到一个加密的方法. 将 $a_1, \cdots, a_n$ 公开, 设 $(m_1, \cdots, m_n)$ 为明文, $m_i = 0$ 或 1, 令

$$s = \sum_{i=1}^{n} m_i a_i,$$

将 s 作为密文, 它是 $a_1, \cdots, a_n$ 的一个部分和. 从 s 求解明文 $(m_1, \cdots, m_n)$ 就相当于解背包问题. 不过对于一般的 $a_1, \cdots, a_n$, 这时合法的收方也同样难于解密, 所以不能用一般的 $a_1, \cdots, a_n$ 设计密码.

在下面一个特殊情况中, 背包问题将变得很容易解, 设

$$a_1 < a_2, \quad a_1 + a_2 < a_3, \cdots, \quad a_1 + a_2 + \cdots + a_{n-1} < a_n,$$

即前面一段数之和小于紧跟其后的一个数, 这时称 $a_1, \cdots, a_n$ 为超递增序列.

设 $a_1, a_2, \cdots, a_n$ 为超递增的, 如以它为公开钥, 以

$$s = \sum_{i=1}^{n} m_i a_i$$

作为明文 $(m_1, \cdots, m_n)$ 的密文, 则任何人都会从 s 解出 $(m_1, \cdots, m_n)$. 所以这样做是不行的, 必须设法将 $a_1, a_2, \cdots, a_n$ 隐藏起来.

取正整数 m, 使 $m > a_1 + a_2 + \cdots + a_n$, 再取正整数 u, 使 u 与 m 互素. u 和 m 作为秘密钥, 只有收方知道. 令

$$b_i \equiv u a_i (\bmod\ m), \quad i = 1, 2, \cdots, n,$$

将 $b_1, b_2, \cdots, b_n$ 作为公开钥, 若 $(m_1, m_2, \cdots, m_n)$ 为明文, 令

$$s = \sum_{i=1}^{n} m_i b_i$$

为密文, 发方将 s 发给收方.

收方利用辗转相除法可以找到 w, 使 $uw \equiv 1(\bmod\ m)$, 因 u 与 m 互素. 他在收到 s 后, 可以算出 $(sw)_0$, 使 $sw \equiv (sw)_0(\bmod\ m)$, 且 $0 < (sw)_0 < m$, 则

$$sw \equiv \sum m_i wua_i \equiv \sum_{i=1}^{n} m_i a_i (\bmod\ m),$$

显然 $\sum m_i a_i < \sum a_i < m$, 可见 $\sum m_i a_i = (sw)_0$, 这是一个超递增背包问题, 很容易解出明文 $(m_1, \cdots, m_n)$.

但后来的研究表明, 这个密码体制是不安全的.

8.5 概率公钥密码

基于定理 3.14, 构造如下的公钥密码 Π. 本节沿用 3.4 节中的符号.

给定正整数 $k \in N'$, k 称为安全参数. 随机选取两个 k 比特的素数 p_1, p_2, 令 $n = p_1 p_2 \in H_k$, 选取一个模 n 的非二次剩余 $y \in \mathbb{Z}_n^1$. 取 (n, y) 为公钥, (p_1, p_2) 为私钥.

加密算法$\boldsymbol{E_n}$ 发方 B 欲将消息 (比特串)$m = m_1 m_2 \cdots m_r$ 发给收方 A, 对每个 $m_i \in \{0, 1\}$, B 随机选取 $x_i \in \mathbb{Z}_n^*$, 若 $m_i = 1$, 则令 $e_i \equiv x_i^2(\bmod\ n)$. 若 $m_i = 0$, 则令 $e_i \equiv yx_i^2(\bmod\ n)$. B 将密文 $E_n(m) = (e_1, e_2, \cdots, e_r)$ 发给 A. 易见, 加密算法的计算量为 $O(rk^2)$.

解密算法$\boldsymbol{D_n}$ 收方掌握私钥 (p_1, p_2), 当他收到密文 $E_n(m) = (e_1, e_2, \cdots, e_r)$ 后, 取 $Q_n(e_i) = m_i$ 就可得到明文 $m = m_1 m_2 \cdots m_r$. 由定理 3.12, $Q_n(e_i)$ 的计算量为 $O(k^3)$, 所以解密算法的计算量为 $O(rk^3)$. 易见 $D_n(E_n(m)) = m$.

明文 m 的密文 $E_n(m) = (e_1, e_2, \cdots, e_r)$ 不是唯一的, 随着 $x_1, x_2, \cdots, x_r$ 不同的选取而变化. 将 Π 称为概率公钥密码. 明文 m 所有可能的密文记为 $E(m)$.

设 $m = m_1 m_2 \cdots m_r$ 和 $m' = m_1' m_2' \cdots m_r'$ 为两个消息, 令 $u = u_1 u_2 \cdots u_r$, 其中 $u_i = m_i m_i'$ $(1 \leqslant i \leqslant r)$ 为一新的消息. 若 $E_n(m') = (e_1', e_2', \cdots, e_r')$, 则

$$\begin{aligned} E_n(u) &= E_n(u_1 u_2 \cdots u_r) = E_n(m_1 m_1', m_2 m_2', \cdots, m_r m_r') \\ &= (e_1 e_1', e_2 e_2', \cdots, e_r e_r') = E_n(m) E_n(m'), \end{aligned}$$

可见加密算法具有同态性质.

可以用以下随机的方法设置密钥参数 $n = p_1 p_2$ 和 y. 随机选取长为 $4k$ 的比特串, 验证它的左边第一个 k 比特串和第两个 k 比特串分别为两个素数的二进制表示, 右边的 $2k$ 比特串为 $\mathbb{Z}_n^1$ 中的一个非二次剩余的二进制表示. 如果上述要求满

足, 则停止搜索. 如果未能满足, 则随机选取另一个 $4k$ 比特串. 利用素数定理、素性检验算法 (见第 9 章), 以及定理 3.12, 可知该算法是一个多项式时间算法.

本节余下部分讨论公钥密码 Π 的安全性.

Π 的潜在攻击方掌握公钥 (n, y), 能够加密任一消息得到相应的密文. 安全参数 k 给定后, 对应的消息集合记为 M_k, M_k 中任一消息的长度约定为 l_k 比特, 这里 $l_k = L(k)$, L 为一多项式.

假定攻击方掌握以下两类运算作为攻击 Π 的工具.

安全参数 k 给定后, 公钥 (n, y) 有很多取法, 以 $C(k)$ 表示所有对应的加密算法的集合.

消息分辨函数 $T = \{T_k\}$, T_k 称为 k 消息分辨函数. 每个 T_k 都是门数为 k 的某个多项式值的布尔函数. 输入 T_k 足够多的比特以刻画随机选取的一个加密算法 $E \in C(k)$, 以及消息 $m \in M_k$ 的一个密文 $\alpha \in E(m)$, T_k 的输出是一个比特 0 或 1. 将 $E(m)$ 中任一密文输入 T_k 时, T_k 输出 1 的概率记为 p_m^E. 设 m_1, $m_2 \in M_k$，若 $|p_{m_1}^E - p_{m_2}^E| > \dfrac{1}{P(k)}$ (P 为多项式), 则称 T_k 关于 E 可以 P-分辨消息 m_1 和 m_2.

消息选择函数 $F = \{F_k\}$, F_k 称为 k 消息选择函数. 每个 F_k 都是门数为 k 的某个多项式值的布尔函数. 输入 F_k 足够多的比特以刻画随机选取的一个加密算法 $E \in C(k)$, F_k 输出两个消息 m_1^k, $m_2^k \in M_k$. $C(k)$ 中的每个加密算法都包含一个 $n \in H_k$, 下文假定对 $C(k)$ 中包含 H_k 中至少 $1/P_1(k)$ (P_1 为多项式) 部分 n 的加密算法, F_k 能生成适合条件 $|p_{n,m_1} - p_{n,m_2}| > 1/P_2(k)$ 的消息 m_1, $m_2 \in M_k$, 这里 $p_{n,m} = p_m^E$, E 为包含 n 的加密算法.

若存在多项式 L, 使对任一 k 有 T_k 的门数 $\leqslant L(k)$, 则称消息分辨函数 $T = \{T_k\}$ 的大小是多项式值有界. 类似地, 定义消息选择函数 $F = \{F_k\}$ 的多项式有界. 简单地说, 一个概率公钥密码是多项式安全, 是指它的任何攻击方不能指望掌握一个多项式有界的消息选择函数, 利用它生成两个消息 m_1 和 m_2, 当得到由 m_1 或者 m_2 加密生成的密文 α 时, 能利用一个多项式有界的消息分辨函数, 以大于 1/2 的概率确定 α 是由 m_1 和 m_2 中那个消息生成的.

可见确定型公钥密码 (如 RSA) 不可能有多项式安全.

更确切地说, 多项式安全的定义如下.

定义 8.1 若 Π 的任一攻击方掌握的消息分辨函数 $T = \{T_k\}$ 的大小是多项式有界. 以 s_k^T 表示它的 k 消息选择函数 F_k 的最小门数. 若对任一多项式 $L(k)$, 当 k 足够大时有 $s_k^T > L(k)$, 则称 Π 具有多项式安全.

定理 8.1 上述基于二次剩余假设定义的概率公钥密码具有多项式安全.

证明 假定消息选择函数 $F = \{F_k\}$ 的大小也是多项式有界, 下文将基于 T 和 F 构造一个函数 $G(n, x)$ ($n \in H_k$, $x \in \mathbb{Z}_n^1$), 对于 H_k 中至少 $1/P_1(k)$ 部分的 n,

$G(n,x)$ 是 $Q_n(x)$ 的 $1/P_2(k)$-逼近, 且 G 的大小多项式有界, 这与 $B = \bigcup_{k\in N'} \{Q_n \,|\, n \in H_k\}$ 是不可逼近 (定理 3.14) 矛盾, 所以 Π 具有多项式安全.

令

$$\varepsilon_k = \frac{1}{P_1(k)}, \quad \mu_k = \frac{1}{P_2(k)},$$

按假设条件, F_k 能生成适合条件

$$|p_{n,m_1} - p_{n,m_2}| > \mu_k$$

的信息 m_1, m_2, n 至少跑遍 H_k 中 $1/P_1(k)$ 部分.

m_1和m_2都为长度l_k的比特串, 假设它们的 Hamming 距离为Δ. 取 a_0, a_1, $\cdots$, a_Δ 为长度 l_k 的比特串, 其中 $a_0 = m_1$, $a_\Delta = m_2$, 任一对相邻的 a_j 和 a_{j+1} $(0 \leqslant j < \Delta)$ 的 Hamming 距离都为 1, 则一定可以找到 x $(0 \leqslant x \leqslant \Delta - 1)$, 使

$$|p_{n,a_x} - p_{n,a_{x+1}}| > \mu_k/l_k.$$

假设 $s = (s_1,\ s_2,\ \cdots,\ s_{l_k})$ 和 $t = (t_1,\ t_2,\ \cdots,\ t_{l_k})$ 为一对相邻的点, 它们的坐标仅在第 d 位不同, 利用 k 消息分辨函数 T_k 分别计算 $p_{n,s}$ 和 $p_{n,t}$, 不妨假设 $p_{n,s} > p_{n,t}$.

假设 $\mathbb{Z}_n^1$ 和 $(\mathbb{Z}_n^1)^{l_k}$ 都具有均匀分布. 对任一 $x = (x_1, x_2, \cdots, x_{l_k}) \in (\mathbb{Z}_n^1)^{l_k}$, 令

$$\mathrm{Sig}(x) = (Q_n(x_1), Q_n(x_2), \cdots, Q_n(x_{l_k})).$$

情况 1　$s_d = 1$, $t_d = 0$.

在符合条件 $Q_n(e_j) = s_j = t_j$ $(j \neq d)$ 及 $e_d = g \in \mathbb{Z}_n^1$ 的所有 $e = (e_1, e_2, \cdots, e_{l_k})$ 中随机选取 $x = (x_1, x_2, \cdots, x_{l_k})$. 若 $T_k(x) = 1$, 令 $G(n,g) = 1$; 若 $T_k(x) = 0$, 令 $G(n,g) = 0$.

情况 2　$s_d = 0$, $t_d = 1$. 令 $G(n,x) = 1 - T_k(x)$. 当 g 跑遍 $\mathbb{Z}_n^1$ 时, 函数 $G(n,g)$ 完成构造.

在情况 1 中, 则有

$$\begin{aligned}
&\Pr(G(n,g) = Q_n(g) \,|\, g \in \mathbb{Z}_n^1)\\
=&\sum_{c=0}^{1} \Pr(G(n,g) = c \,|\, Q_n(g) = c)\Pr(Q_n(g) = c)\\
=&\frac{1}{2}\Big[\Pr(G(n,g) = 1 \,|\, Q_n(g) = 1) + \Pr(G(n,g) = 0 \,|\, Q_n(g) = 0)\Big]\\
=&\frac{1}{2}\Big[\Pr(T_k(x) = 1 \,|\, \mathrm{Sig}(x) = s) + \Pr(T_k(x) = 0 \,|\, \mathrm{Sig}(x) = t)\Big]\\
=&\frac{1}{2}(p_{n,s} + (1 - p_{n,t})) > \frac{1}{2} + \frac{\mu_k}{2l_k}.
\end{aligned}$$

可见对于 H_k 中至少 ε_k 部分的 n, $G(n,g)$ 是 $Q_n(g)$ 的 $(\mu_k/2l_k)$-逼近, 由于 T 和 F 的大小都是多项式有界, 所以基于 T 和 F 构造的函数 G 的大小也是多项式有界, 这与定理 3.14 的结论矛盾.

关于情况 2, 也可以类似地证明.

定理 8.1 的证明可参考文献 [18] 中 5.2 节的定理 5.1. 这里的证明作了简化.

在使用以上定义的公钥密码时, 当消息长为 r 比特时, 对应的密文长为 $2kr$ 比特, 增加 $2k$ 倍. Blum 和 Goldwasser 在文献 [5] 中提出了另一个概率公钥密码, 密文的长度是消息长度再加一个固定的长度.

8.6 秘密共享

一个机密数据 K(如密钥), 交给一个人保管, 一旦丢失或 "泄露", 就会造成严重后果. 如果同时让几个人都保管, 则减少了丢失的可能性, 但增加了泄露的可能性, 所以理想的办法是用某种方法将秘密分成几部分, 由几个人分别保管其中一部分, 只有当这些人或其中一部分人都同意时, 将他们保管的部分凑在一起, 才能得到机密数据 K. 这就是秘密共享的思想.

设有 n 个人参与一个秘密共享方案. 把分发给每个参与者保管的秘密数称为是分配给他的信息片. 考虑一个简单的秘密共享方案, 假设任意 s 个参与者的信息片凑在一起就能得出 K, 而任意不足 s 个参与者的信息片凑在一起不能确定 K, 称这方案为 (s,n) 门限方案. 本节利用孙子定理给出一个构造 (s,n) 门限方案的方法.

取素数 p, 使 $K<p$, 取两两互素的正整数 $m_1,m_2,\cdots,m_n$ 都与 p 互素, 且

$$\begin{aligned} &m_1<m_2<\cdots<m_n,\\ &m_1m_2\cdots m_s>pm_nm_{n-1}\cdots m_{n-s+2}, \end{aligned} \tag{8.2}$$

令 $M=m_1m_2\cdots m_s$, 式 (8.2) 表明 M/p 比 $m_1,\cdots,m_n$ 中任意 $s-1$ 个数的乘积都大.

任取非负整数 $t<M/p-1$, 令

$$K_0=K+tp,$$

则 $0\leqslant K_0=K+tp<(1+t)p\leqslant(M/p)p=M$, 取

$$k_j\equiv K_0\,(\mathrm{mod}\ m_j),\quad j=1,2,\cdots,n,$$

以 $k_1,k_2,\cdots,k_n$ 作为分配给每个参与者的信息片, 利用上述方法就定义了一个 (s,n) 门限方案. 选择不同的 t, 可产生不同的信息片.

若已知任意 s 个参与者的信息片 $k_{j_1}, k_{j_2}, \cdots, k_{j_s}$, 由同余方程组

$$K_0 \equiv k_{j_i} (\text{mod } m_{j_i}), \quad i = 1, 2, \cdots, s,$$

利用孙子定理, 可求出 K_0 模 $M_j = m_{j_1} m_{j_2} \cdots m_{j_s}$ 的最小正剩余 a, 即

$$K_0 \equiv a (\text{mod } M_j), \quad 0 \leqslant a < M_j,$$

但由于 $0 \leqslant K_0 < M \leqslant M_j$, 故 $K_0 = a$, 进而 $K = K_0 - tp$, 即由 $k_{j_1}, k_{j_2}, \cdots, k_{j_s}$ 可确定 K.

若仅知道 $s-1$ 个参与者的信息片 $k_{j_1}, \cdots, k_{j_{s-1}}$, 记 $M' = k_{j_1} \cdots k_{j_{s-1}}$, 由同余方程组

$$K_0 \equiv k_{j_i} (\text{mod } m_{j_i}), \quad i = 1, 2, \cdots, s-1,$$

可知 $K_0 \equiv a (\text{mod } M')$, $0 \leqslant a < M'$, 因而

$$K_0 = a + xM', \quad 0 \leqslant x < M/M',$$

由式 (8.2) 可知 $p < M/M'$, 所以 x 可跑遍 $0 \leqslant x < p$. M' 与 p 互素, 可见 xM' 可跑遍模 p 的剩余类, K_0 也可跑遍模 p 的剩余类, 由 K_0 不能确定 $K (= K_0 - tp)$. 所以任意不足 s 个参与者的信息片不能确定 K, 利用上述方法确实得到了一个 (s, n) 门限方案.

例 若$K = 4$, 来给出一个$(2, 3)$ 门限方案. 取 $p = 7, m_1 = 11, m_2 = 12, m_3 = 17$, 则 $M = m_1 m_2 = 132 > pm_3 = 119$, 这时 $M/p = 132/7$, 任取 $t = 14 < M/p$, 这时

$$K_0 = K + tp = 4 + 14 \times 7 = 102$$

分配给三个参与者的信息片分别为

$$\begin{aligned} k_1 &\equiv 102 \equiv 3 \, (\text{mod } 11), \\ k_2 &\equiv 102 \equiv 6 \, (\text{mod } 12), \\ k_3 &\equiv 102 \equiv 0 \, (\text{mod } 17), \end{aligned}$$

即 $k_1 = 3, k_2 = 6, k_3 = 0$.

第 9 章　素 性 检 验

9.1　Fermat 小定理及伪素数

给定一个自然数 n, 判断 n 是不是素数, 称为素性检验.

若 n 是素数, 整数 a 与 n 互素, 由 Fermat 小定理可知

$$a^{n-1} \equiv 1 (\bmod\ n). \tag{9.1}$$

如果能够找到一个与 n 互素的整数 a, 使式 (9.1) 不成立, 则可断定 n 是复合数. 但相反结论并不能成立, 即当式 (9.1) 成立时, 并不能断定 n 是素数. 实际上, 存在这样的复合数 n, 能使式 (9.1) 对任意与其互素的 a 都成立. 我们称这样的复合数为 Carmichael 数.

当式 (9.1) 成立时, n 称为以 a 为基的伪素数.

在计算模 n 的方幂 $a^u (\bmod\ n)$ 时, 将 u 表成二进制

$$u = \alpha_0 + \alpha_1 \cdot 2 + \alpha_2 \cdot 2^2 + \cdots + \alpha_t \cdot 2^t, \quad \alpha_i = 0 \text{ 或 } 1,$$

将 a 逐次平方得 $a^2, (a^2)^2 = a^{2^2}, a^{2^3}, \cdots, a^{2^t} (\bmod\ n)$, 然后将对应 $\alpha_i = 1$ 的那些方幂 a^{2^i} 连乘, 并模 n.

设 $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ 为 Carmichael 数, 存在整数 a_0, 使

$$a_0 \equiv q_i (\bmod\ p_i^{r_i}), \quad i = 1, 2, \cdots, t,$$

其中 q_i 为模 $p_i^{r_i}$ 的原根. a_0 模 n 的阶为

$$\begin{aligned} d =& [\varphi(p_1^{r_1}), \varphi(p_2^{r_2}), \cdots, \varphi(p_t^{r_t})] \quad (\text{最小公倍数}) \\ =& [p_1^{r_1-1}(p_1-1), p_2^{r_2-1}(p_2-1), \cdots, p_t^{r_t-1}(p_t-1)], \end{aligned}$$

因 n 为 Carmichael 数, 故 $d | n-1$.

若 $r_i > 1$, 则 $p_i | d$, 但 $p_i \nmid n-1$, 故对一切 i 有 $r_i = 1$, 即 n 没有重因子.

若 $t = 2$, 则 $p_1 - 1 | p_1 p_2 - 1$. 由于 $p_1 p_2 - 1 = (p_1 - 1) p_2 + p_2 - 1$, 故 $p_1 - 1 | p_2 - 1$. 同理, 有 $p_2 - 1 | p_1 - 1$, 因而 $p_1 - 1 = p_2 - 1$, 这不可能, 即 n 至少是三个素因子的乘积.

式 (9.1) 成立的充分必要条件是 a 模 n 的阶是 $n-1$ 的因子, a 模 n 的阶一定是 d 的因子, 且一定存在一个 a, 使它的阶等于 d, 可见 $d|n-1$ 是 n 为 Carmichael 数的充分必要条件. 当 $n=p_1p_2\cdots p_t$ 时, 当且仅当 $p_i-1|n-1(i=1,2,\cdots,t)$, n 为 Carmichael 数.

下列这些都是 Carmichael 数:

$$\begin{aligned}&3\cdot 11\cdot 17=561, \quad 5\cdot 13\cdot 17=1105, \quad 7\cdot 13\cdot 19=1729, \quad 5\cdot 17\cdot 29=2465,\\ &7\cdot 13\cdot 31=2821, \quad 7\cdot 23\cdot 41=6601, \quad 13\cdot 37\cdot 61=29341, \quad 7\cdot 13\cdot 31\cdot 61=172081.\end{aligned}$$

虽然 Fermat 小定理没有直接给出素性检验的一个有效算法, 但是很多素性检验的算法都是从它发展出来的.

9.2 强伪素数及 Miller-Rabin 检验

当 n 为素数, a 与 n 互素时, 将同余式

$$a^{n-1}\equiv 1\,(\bmod\ n)$$

两端逐次开方, 可得

$$a^{\frac{n-1}{2}}, \quad a^{\frac{n-1}{4}},\cdots, \quad a^{\frac{n-1}{2^s}}$$

$\left(\text{设} 2\nmid \dfrac{n-1}{2^s}\right)$, 则第一个模 n 不等于 1 的数必为模 n 等于 -1, 因为当 n 为素数时, 仅有 ± 1 的平方模 n 为 1, 由此引入下面的定义.

定义 9.1 *设 $n-1=2^st$, $2\nmid t$, b 与 n 互素, 若*

$$b^t\equiv 1\,(\bmod\ n) \quad \text{或} \quad \exists r,\ 0\leqslant r<s \text{ 使 } b^{2^rt}\equiv -1\,(\bmod\ n), \tag{9.2}$$

则称 n 是以 b 为基的强伪素数.

由上述, 当 n 为素数时, 它一定是以任何数 b(b与n互素) 为基的强伪素数, 以 b 为基的强伪素数, 一定是 9.1 节所定义的以 b 为基的伪素数.

定理 9.1 *若 n 是奇的复合数, 则在区间 $0<b<n$ 中, 最多有 25% 个数 b, 能使 n 是以 b 为基的强伪素数.*

在证明定理 9.1 之前, 先来介绍 Miller-Rabin 检验. 在 0 与 n 间任取 b, 计算 $b^t(\bmod\ n)$, 若为 ± 1, 则称 n 通过检验式 (9.2), 否则依次计算 $b^{2t}, b^{4t},\cdots, b^{2^{s-1}t}(\bmod\ n)$, 如果能得到 -1, 则称 n 通过检验式 (9.2), 如果不能得到 -1, 则称 n 对该 b 不能通过检验式 (9.2), 这时可以肯定 n 为复合数. 如果随机选取 k 个 $b(0<b<n)$, 而 n 对这 k 个 b 都能通过检验式 (9.2), 由定理 9.1, 可知此事

件发生的可能性小于 $1/4^k$, 可以认为这时 n 为复合数的可能性小于 $1/4^k$. 这就是 Miller-Rabin 检验.

为了证明定理 9.1, 需要两个引理.

引理 9.1 　*在 m 阶循环群中, $x^k=1$ 的解的个数为 (m,k).*

证明 　设 g 为循环群的生成元, 则 $1,g,g^2,\cdots,g^{m-1}$ 即为整个群, 若 $g^{jk}=1$, 则$m|jk$. 记 $d=(m,k)$, 则$\frac{m}{d}\Big|j\frac{k}{d}$. 由于$\frac{m}{d}$与$\frac{k}{d}$互素, 因而 $\frac{m}{d}\Big|j$, j 可取为 $0,\frac{m}{d}$, $2\frac{m}{d},\cdots,(d-1)\frac{m}{d}$, 即方程 $x^k=1$ 有 d 个解, 证毕.

引理 9.2 　*设 p 为奇素数, $p-1=2^{s'}t'$, $2\nmid t'$, 则同余式*

$$x^{2^rt}\equiv -1\,(\bmod\ p),\quad 2\nmid t$$

的解数为

$$u=\begin{cases}0, & r\geqslant s',\\ 2^r(t,t'), & r<s'.\end{cases}$$

证明 　设 g 为模 p 的原根, 若

$$g^{j\cdot 2^rt}\equiv -1\,(\bmod\ p),$$

由于 $g^{\frac{(p-1)}{2}}\equiv -1(\bmod\ p)$, 故 $g^{2^rtj-2^{s'-1}t'}\equiv 1(\bmod\ p)$, 所以

$$2^rtj\equiv 2^{s'-1}t'\,(\bmod\ 2^{s'}t'),$$

这里 j 作为未定元. 当 $r\geqslant s'$ 时, 该同余方程对 j 无解; 当 $r<s'$ 时,

$$j\cdot\frac{t}{(t,t')}\equiv 2^{s'-1-r}\frac{t'}{(t,t')}\left(\bmod\ \frac{2^{s'-r}t'}{(t,t')}\right),$$

由于 $\frac{t}{(t,t')}$ 与 $2^{s'-r}t'/(t,t')$ 互素, j 模 $2^{s'-r}t'/(t,t')$ 有唯一解, 所以模 $p-1$ 有

$$\frac{2^{s'}t'}{2^{s'-r}t'(t,t')^{-1}}=2^r(t,t')$$

个解.

定理 9.1 的证明 　分别考虑三种情况:

(1) n 含平方因子. 设 $p^\alpha\|n,\alpha\geqslant 2$, 这时可以证明, 能使 n 成为以 b 为基的伪素数的 b 在区间 $(0,n)$ 中不超过 25%. 设 $b^{n-1}\equiv 1(\bmod\ n)$, 则 $b^{n-1}\equiv 1(\bmod\ p^2)$, $(\mathbb{Z}/p^2\mathbb{Z})^*$ 是一个 $\varphi(p^2)$ 阶循环群, 由引理 9.1 , 在区间 $(0,p^2)$ 中, 有 $d=(p(p-$

$1), n-1)$ 个 b 适合 $b^{n-1} \equiv 1 (\bmod\ p^2)$. 由于 $p \nmid n-1$, 所以 $d \leqslant p-1$. 在区间 $(0, n)$ 内, 能使 $b^{n-1} \equiv 1 (\bmod\ p^2)$ 成立的 b 的个数可占比例不超过

$$\frac{p-1}{p^2-1} = \frac{1}{p+1} \leqslant \frac{1}{4}.$$

(2) $n = pq$ 为两个素数之积. 设 $p-1 = 2^{s'}t', q-1 = 2^{s''}t'', t'$与$t''$ 为奇数, 记 $n-1 = 2^s t$, t 也为奇数. 不妨设 $s' \leqslant s''$, 若 n 是以 b 为基的强伪素数, 则

(i) $b^t \equiv 1 (\bmod\ p)$, $b^t \equiv 1 (\bmod\ q)$; 或

(ii) 存在 $0 \leqslant r < s$, 使 $b^{2^r t} \equiv -1 (\bmod\ p)$, $b^{2^r t} \equiv -1 (\bmod\ q)$.

由引理 9.1, 使 (i) 成立的 b 的个数为 $(t, t')(t, t'') \leqslant t't''$. 由引理 9.2, 对任一 $r < \min(s', s'') = s'$, 使 (ii) 成立的 b 的个数为

$$2^r (t, t') \cdot 2^r (t, t'') \leqslant 4^r t' t'',$$

由于 $n-1 > \varphi(n) = (p-1)(q-1) = 2^{s'+s''} t' t''$, 所以在区间 $(0, n)$ 内能使 n 成为以 b 为基的强伪素数的 b 所占的比例不超过

$$\frac{t't'' + \sum_{r=0}^{s'-1} 4^r t' t''}{2^{s'+s''} t' t''} = 2^{-s'-s''} \left(1 + \frac{4^{s'}-1}{4-1}\right). \tag{9.3}$$

若 $s' < s''$, 则该比例不超过

$$2^{-2s'-1} \left(\frac{2}{3} + \frac{4^{s'}}{3}\right) \leqslant 2^{-3} \frac{2}{3} + \frac{1}{6} = \frac{1}{4};$$

若 $s' = s''$, 在以上统计所用到的两个不等式

$$(t, t') \leqslant t', \quad (t, t'') \leqslant t''$$

中, 至少有一个是严格的不等式. 否则, 将有 $t' | t$, $t'' | t$. 由于 $2^s t = n-1 = (p-1)q + q - 1 = 2^{s'} t' q + 2^{s''} t''$, 所以 $t' | t''$, 同理, 有 $t'' | t'$, 即 $t' = t''$, 由此可知 $p = q$, 这不可能. 由于 t, t', t'' 都是奇数, 当 $(t, t') < t'$ 时, 至少差一个因子 3, 即 $(t, t') \leqslant \dfrac{1}{3} t'$, 所以

$$(t, t')(t, t'') \leqslant \frac{1}{3} t' t''.$$

这时所求的比例不超过

$$\frac{1}{3} \cdot 2^{-2s'} \left(\frac{2}{3} + \frac{4^{s'}}{3}\right) \leqslant \frac{1}{18} + \frac{1}{9} = \frac{1}{6} < \frac{1}{4}.$$

(3) n 为三个以上的素数之积. 设 $n=p_1p_2\cdots p_k, k\geqslant 3$, $p_i-1=2^{s_i}t_i$, t_i 为奇数. 不妨设 $s_1\leqslant s_j$, 类似与 (2) 中的推论, 在 $(0,n)$ 内, 能使 n 成为以 b 为基的强伪素数的 b 所占的比例不超过

$$\begin{aligned}&2^{-s_1-s_2-\cdots-s_k}\left(1+\frac{2^{ks_1}-1}{2^k-1}\right)\leqslant 2^{-ks_1}\left(\frac{2^k-2}{2^k-1}+\frac{2^{ks_1}}{2^k-1}\right)\\=&2^{-ks_1}\frac{2^k-2}{2^k-1}+\frac{1}{2^k-1}\leqslant 2^{-k}\cdot\frac{2^k-2}{2^k-1}+\frac{1}{2^k-1}=2^{1-k}\leqslant\frac{1}{4},\end{aligned}$$

定理 9.1 证毕.

令 $n-1=2^sw(2\nmid w)$. 在利用 Miller-Rabin 检验时, 首先在区间 $(1,n)$ 内任取一与 n 互素的整数 b, 计算 $b^w(\bmod n)$, 若 $b^w\equiv\pm 1(\bmod n)$, 则 n 是以 b 为基的强伪素数. 否则, 依次计算 b^{2w}, b^{4w}, $\cdots$, $b^{2^{s-1}w}$, 若其中某个数为 $-1(\bmod n)$, 则 n 是以 b 为基的强伪素数; 若其中某个数 $\neq\pm 1(\bmod n)$, 而其平方 (即其后相邻之数)$\equiv 1(\bmod n)$, 则 n 一定是合数. 在 $(1,n)$ 中随机抽取 T 个与 n 互素的数, 若 n 是以其中每个数为基的强伪素数, 则判断 n 为素数, 由定理 9.1, 可知判断错误的概率为 4^{-T}.

9.3　利用 $n-1$ 的因子分解的素性检验

如果能将 $n-1$ 完全分解为素因子乘积, 则有以下的一个确定型的素性检验.

定理 9.2　*设存在一整数 a 适合*

$$\begin{cases}a^{n-1}\equiv 1\,(\bmod n),\\ \text{对 } n-1 \text{ 的任一素因子 } p, \text{ 有 } a^{\frac{n-1}{p}}\not\equiv 1\,(\bmod n),\end{cases}$$

则 n 为素数.

证明　由定理中所给的第一个条件可知 a 与 n 互素, 第两个条件即是说 a 模 n 的阶为 $n-1$. 由 a 的乘方可产生 $1,2,\cdots,n-1(\bmod n)$ 共 $n-1$ 个数, 它们与 n 都互素, 可见 n 为素数.

如果仅能将 $n-1$ 分解一部分, 即若 $n-1=ab$, b 能完全分解为素数乘积, 当 $0<a\leqslant b+1$ 时 (即当 $b>\sqrt{n-1}$ 时), 有如下的定理.

定理 9.3(Pocklinton)　*设 $n=ab+1>1$, $0<a\leqslant b+1$, 若对 b 的任一素因子 p 都存在一整数 x, 使 $x^{n-1}\equiv 1(\bmod n)$ 及 $\gcd(x^{(n-1)/p}-1,n)=1$, 则 n 是素数.*

证明　因已知 b 的所有素因子, 不妨假设 a 与 b 互素. 用反证法, 假设 n 有素因子 q, 且 $q\leqslant\sqrt{n}$. 对 b 的每个素因子 p, 存在整数 x_p, 使 $x_p^{n-1}\equiv 1(\bmod q)$, $x_p^{(n-1)/p}\not\equiv 1(\bmod q)$, 即

$$\operatorname{ord}_q(x_p)|n-1,\quad \operatorname{ord}_q(x_p)\nmid\frac{n-1}{p}.$$

若 $p^k||b$, 可知 $\mathrm{ord}_q(x_p)=sp^k$, 因而 $\mathrm{ord}_q(x_p^a)|b, \mathrm{ord}_q(x_p^a)\nmid \dfrac{b}{p}$. 令

$$x=\prod_{p|b} x_p^a,$$

可见 $\mathrm{ord}_q(x)=b$, 由此推出 $q-1\geqslant b$ 及

$$q^2\geqslant (b+1)^2\geqslant a(b+1)=ab+a\geqslant n,$$

因而 $q^2=n$(因 $q\leqslant\sqrt{n}$), $a=b+1, a=1$, 矛盾, 证毕.

定理 9.4(Proth) 设 $3\nmid k$, $k\leqslant 2^n+1$, $3<2^n+1$, 则下列条件等价:

(1) $k\cdot 2^n+1$ 是素数;

(2) $3^{k\cdot 2^{n-1}}\equiv -1(\mathrm{mod}\ k\cdot 2^n+1)$.

证明 (2) $\Longrightarrow$ (1) 在定理 9.3 中, 取 $a=k, b=2^n$, 以及 $x=3$, 则 $3^{ab}=3^{k\cdot 2^n}\equiv 1(\mathrm{mod}\ k\cdot 2^n+1)$, $3^{k\cdot 2^{n-1}}\equiv -1(\mathrm{mod}\ k\cdot 2^n+1)$, 利用定理 9.3, 可知 $k\cdot 2^n+1$ 为素数.

(1) $\Longrightarrow$ (2) 因 $3\nmid k$, $k\cdot 2^n+1$ 为素数, 所以一定有 $k\cdot 2^n+1\equiv 2(\mathrm{mod}\ 3)$, 利用二次互反律得

$$\left(\frac{3}{k\cdot 2^n+1}\right)=(-1)^{k\cdot 2^{n-1}}\left(\frac{k\cdot 2^n+1}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

可知 (2) 成立.

记 $F_n=2^{2^n}+1$ 为第 n 个 Fermat 数, 由定理 9.4 可知下述两条件等价:

(1) F_n 为素数;

(2) $3^{(F_n-1)/2}\equiv -1(\mathrm{mod}\ F_n)$.

9.4 利用 $n+1$ 的因子分解的素性检验

取 P, Q 两个整数, 定义序列

$$u_0=0,\quad u_1=1,\cdots,\quad u_{k+2}=Pu_{k+1}-Qu_k\quad (k\geqslant 0),$$

称为 Lucas 序列. 令

$$S=\sum_{i=0}^{\infty} u_i x^i,$$

易见

$$(1-Px+Qx^2)S=x,$$

因而

$$S = \frac{x}{1 - Px + Qx^2},$$

设 $x^2 - Px + Q$ 的两个根为 α, β, 则有

$$\alpha + \beta = P, \quad \alpha\beta = Q,$$

以及

$$1 - Px + Qx^2 = (1 - \alpha x)(1 - \beta x),$$

所以

$$S = \frac{x}{(1 - \alpha x)(1 - \beta x)} = \frac{1}{\alpha - \beta}\Big(\frac{1}{1 - \alpha x} - \frac{1}{1 - \beta x}\Big) = \sum_{i=0}^{\infty} \frac{\alpha^i - \beta^i}{\alpha - \beta} x^i,$$

比较两端 x^i 的系数可得

$$u_i = \frac{\alpha^i - \beta^i}{\alpha - \beta}, \quad i = 0, 1, \cdots .$$

由于 $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = P^2 - 4Q$, 令 $\Delta = P^2 - 4Q$, Δ 称为序列 $\{u_i\}$ 的判别式, 则有 $\alpha - \beta = \sqrt{\Delta}$.

不妨设 Δ 无平方因子 (若设 Δ 不是完全平方数, 下述讨论亦真), $\Delta \neq 1$, 这时 $\Delta \equiv 1 (\mathrm{mod}\ 4)$, 集合

$$O = \left\{ \frac{a + b\sqrt{\Delta}}{2} \middle| a, b \in \mathbb{Z}, a \equiv b (\mathrm{mod}\ 2) \right\}$$

是二次域 $\mathbb{Q}(\sqrt{\Delta})$ 中的代数整数环. 设 M 为 O 中的理想, O 中两个元素 u, v 若适合 $u - v \in M$, 则记为 $u \equiv v (\mathrm{mod}\ M)$.

定理 9.5 设 n 为奇数, $(n, \Delta Q) = 1$. 又设 q 为奇素数, 且 $q \nmid \Delta Q$, 则

(1) $\alpha, \beta, \alpha - \beta$(在 O 中) 模 n 可逆;

(2) $u_k \equiv 0 (\mathrm{mod}\ n) \iff (\alpha\beta^{-1})^k \equiv 1 (\mathrm{mod}\ n)$, 这里 β^{-1} 表示 O 中适合 $\beta\beta^{-1} \equiv 1 (\mathrm{mod}\ n)$ 的元素;

(3) 若 $r \in O$, 则

$$r^q \equiv \begin{cases} r\,(\mathrm{mod}\ q), & \left(\dfrac{\Delta}{q}\right) = 1, \\ \widetilde{r}\,(\mathrm{mod}\ q), & \left(\dfrac{\Delta}{q}\right) = -1, \end{cases}$$

$\widetilde{r}$ 表示 r 在 O 中的共轭元.

(4)

$$u_{q-1} \equiv 0 \,(\bmod\, q), \quad \left(\frac{\Delta}{q}\right) = 1,$$
$$u_{q+1} \equiv 0 \,(\bmod\, q), \quad \left(\frac{\Delta}{q}\right) = -1.$$

证明 (1) 由于 $(n,Q)=1$, $\exists\omega\in\mathbb{Z}$, 使$Q\omega\equiv 1(\bmod n)$, 所以在 O 中有 $\alpha\beta\omega = Q\omega \equiv 1(\bmod n)$(这表示 $\alpha\beta\omega - 1 \in n\cdot O$) , 可见 $\beta\omega(\bmod n)$ 是 $\alpha(\bmod n)$ 的逆, $\alpha\omega(\bmod n)$ 是 $\beta(\bmod n)$ 的逆. 由于 $\alpha-\beta = \sqrt{\Delta}$, 故 $(\alpha-\beta)^{2\varphi(n)} = \Delta^{\varphi(n)} \equiv 1(\bmod n)$, 所以 $(\alpha-\beta)^{2\varphi(n)-1}$ 是 $(\alpha-\beta)(\bmod n)$ 的逆.

(2) 因 $u_k = (\alpha^k-\beta^k)/(\alpha-\beta)$, $\alpha-\beta$ 模 n 可逆, 所以 $u_k\equiv 0(\bmod n) \Longleftrightarrow \alpha^k \equiv \beta^k \ (\bmod n) \Longleftrightarrow (\alpha\beta^{-1})^k \equiv 1(\bmod n)$.

(3) 设 $r = \dfrac{a+b\sqrt{\Delta}}{2}$, 因而

$$\begin{aligned}2r^q \equiv 2^q r^q &= (2r)^q = (a+b\sqrt{\Delta})^q \,(\bmod\, q)\\ &\equiv a^q + b^q\Delta^{q/2} = a + b\sqrt{\Delta}\cdot\Delta^{\frac{q-1}{2}} \,(\bmod\, q)\\ &\equiv a + b\left(\frac{\Delta}{q}\right)\sqrt{\Delta}\,(\bmod\, q),\end{aligned}$$

所以

$$r^q \equiv \frac{a+b\left(\dfrac{\Delta}{q}\right)\sqrt{\Delta}}{2} = \begin{cases} r, & \left(\dfrac{\Delta}{q}\right)=1,\\ \widetilde{r}, & \left(\dfrac{\Delta}{q}\right)=-1.\end{cases}$$

(4) 若 $\left(\dfrac{\Delta}{q}\right) = 1$, 则由 (3), $\alpha^{q-1}\equiv 1(\bmod q)$. 同样地, $\beta^{q-1}\equiv 1(\bmod q)$. 所以 $(\alpha\beta^{-1})^{q-1}\equiv 1(\bmod n)$, 由 (2) 得到 $u_{q-1}\equiv 0(\bmod q)$.

若 $\left(\dfrac{\Delta}{q}\right) = -1$, 则由 (3) 可知

$$\alpha^{q+1} = \alpha^q\cdot\alpha \equiv \widetilde{\alpha}\alpha = \beta\alpha = \beta\widetilde{\beta} \equiv \beta\beta^q = \beta^{q+1}(\bmod q),$$

因而 $(\alpha\beta^{-1})^{q+1}\equiv 1(\bmod q)$, 由 (2)得 $u_{q+1}\equiv 0(\bmod q)$(因为 α,β 为方程 $x^2-Px+Q=0$ 的两个根, 故有 $\widetilde{\alpha}=\beta$), 证毕.

利用定理 9.5, 得到如下的 Lucas-Lehmer 素性检验.

定理 9.6 设 n 为奇数, $\Delta\equiv 1(\bmod 4)$, $\Delta = P^2-4Q$ 及 $(n,\Delta Q)=1$. 若 $u_{n+1}\equiv 0(\bmod n)$, 且对 $n+1$ 的任一素因子 q, 有 $(u_{(n+1)/q}, n) = 1$, 则 n 为素数.

证明 设 r 为 n 的一个素因子, $r\neq n$, 仍令 α,β 为 $x^2-Px+Q=0$ 的两个根, 设 k 为最小正整数, 使 $(\alpha\beta^{-1})^k\equiv 1(\bmod r)$. 因 $u_{n+1}\equiv 0(\bmod r), u_{(n+1)/q}\not\equiv$

$0 \pmod r$), 由定理 9.5 的 (2), 可知 $k|n+1, k\nmid \frac{n+1}{q}$, 这里 q 是可为 $n+1$ 的任一素因子, 故 $k=n+1$, 由定理 9.5 的 (4), 有 $u_{r\pm1}\equiv 0 \pmod r$)($\pm1$ 选其中一个). 因此 $(\alpha\beta^{-1})^{r\pm1}\equiv 1 \pmod r$), 所以 $n+1|r\pm1$, 这是不可能的, 故 n 为素数, 证毕.

9.5　分圆环素性检验

本节介绍基于代数数论的一个素性检验方法, 称作 “分圆环” 素性检验. 其主要思想是: 基于在分圆环中的一些恒等式, 若 n 是素数, 这些恒等式是对的; 若 n 是合数, 这些恒等式均成立的可能性很小. 事实上, 当验证了所有这些恒等式后, 可以得到一些关于 n 的素因子的额外信息, 确切地说, 将证明 n 的所有素因子必须落在一个相当小的同余类中, 而这点是容易验证的.

设 n 是待检验的奇数, p, q 是两个互不相同的素数, 且 $p\nmid n$, $q\nmid n$, $p|q-1$, 令 ξ_p, ξ_q 分别是复数域 $\mathbb{C}$ 中的 p 次、q 次本原单位根, g 是 $\mathbb{Z}_q^*$ 的一个生成元, 定义一个特征函数:

$$\chi_{p,q}:\begin{cases}\mathbb{Z}_q^*\longrightarrow\mathbb{C}^*,\\ g^i\longmapsto\xi_p^i.\end{cases}$$

显然, $\chi\overset{\triangle}{=}\chi_{p,q}$ 是一个群同态. χ伴随着另一个群同态 $\bar\chi(g^i\to\xi_p^{-i}=\xi_p^{p-i})$, 即 $\bar\chi(a)=\chi(a)^{-1}$. 定义特征和

$$\tau(\chi)=\sum_{1\leqslant a\leqslant q-1}\chi(a)\xi_q^a\in\mathbb{Z}[\xi_p,\xi_q].$$

引理 9.3　$\tau(\chi)\cdot\tau(\bar\chi)=\chi(-1)q$.

证明　因为 $\sum\limits_{1\leqslant a\leqslant q-1}\chi(a)=0$, 且

$$\sum_{i=1}^{q-1}\xi_q^{ki}=\begin{cases}q-1, & k\equiv 0\pmod q,\\ -1, & k\not\equiv 0\pmod q,\end{cases}$$

所以

$$\begin{aligned}\tau(\chi)\cdot\tau(\bar\chi)&=\left(\sum_{1\leqslant a\leqslant q-1}\chi(a)\xi_q^a\right)\cdot\left(\sum_{1\leqslant b\leqslant q-1}\bar\chi(b)\xi_q^b\right)\\&=\sum_{1\leqslant a,b\leqslant q-1}\chi(a)\cdot\bar\chi(b)\xi_q^{a+b}=\sum_{1\leqslant a,b\leqslant q-1}\chi(ab)\cdot\bar\chi(b)\xi_q^{ab+b}\\&=\sum_{1\leqslant a\leqslant q-1}\chi(a)\sum_{1\leqslant b\leqslant q-1}\xi_q^{b(a+1)}=\chi(q-1)(q-1)-\sum_{1\leqslant a\leqslant q-2}\chi(a)\\&=\chi(-1)(q-1)+\chi(-1)=\chi(-1)q.\end{aligned}$$

引理 9.4 令 $R=\mathbb{Z}[\xi_p,\xi_q]$, 若 n 是素数, 那么 $\tau(\chi)^{n^{p-1}-1}\equiv\chi(n)(\bmod nR)$.

证明 因 $\chi(a)$ 是 p 次单位根, 且 $n^{p-1}\equiv 1(\bmod p)$, 所以 $\chi(a)=\chi(a)^{n^{p-1}}$, 故

$$\begin{aligned}\tau(\chi)^{n^{p-1}}&=\left(\sum_{1\leqslant a\leqslant q-1}\chi(a)\xi_q^a\right)^{n^{p-1}}\\&\equiv\sum_{1\leqslant a\leqslant q-1}\chi(a)^{n^{p-1}}\xi_q^{an^{p-1}}\\&=\sum_{1\leqslant a\leqslant q-1}\chi(a)\cdot\xi_q^{an^{p-1}}\,(\bmod nR).\end{aligned}$$

令 $b=(n^{p-1})^{-1}(\bmod q)$, 那么

$$\begin{aligned}\tau(\chi)^{n^{p-1}}&=\sum_{1\leqslant a\leqslant q-1}\chi(ab)\xi_q^{(a\cdot b)n^{p-1}}\,(\bmod nR)\\&=\chi(b)\sum_{1\leqslant a\leqslant q-1}\chi(a)\xi_q^a\\&=\chi(b)\cdot\tau(\chi)\\&=\chi(n)^{1-p}\tau(\chi)\\&=\chi(n)\tau(\chi).\end{aligned}$$

可知 $\tau(\chi)^{n^{p-1}-1}\equiv\chi(n)(\bmod nR)$.

引理 9.4 是 Fermat 小定理在分圆环上的推广, 若取 $p=2$, 则

$$\tau(\chi)^{n-1}\equiv\chi(n)(\bmod nR),$$

意味着 $\left(\tau(\chi)^2\right)^{\frac{n-1}{2}}=\pm 1(\bmod nR)$, 再由引理 9.3 知

$$(\chi(-1)q)^{\frac{n-1}{2}}=\pm 1(\bmod nR),$$

即 $q^{\frac{n-1}{2}}=\pm 1(\bmod n)$.

引理 9.5 设 r 为素数, $r\neq p$, 若 $\xi_p^i\equiv\xi_p^j(\bmod r\mathbb{Z}[\xi_p])$, 那么 $\xi_p^i=\xi_p^j$.

证明 只需证由 $\xi_p^k\equiv 1(\bmod r\mathbb{Z}[\xi_p])$ 可得 $\xi_p^k=1$.

令 $\Phi_p(x)=x^{p-1}+\cdots+x+1$ 是 ξ_p 的极小多项式, 那么

$$\Phi_p\left(\xi_p^k\right)\equiv\Phi_p(1)=p\not\equiv 0\,(\bmod r\mathbb{Z}[\xi_p]),$$

ξ_p^k 不能是 p 次本原单位根, 所以 $\xi_p^k=1$.

令 P 和 Q 均是由一些不整除 n 的素数构成的集合, 且满足对任意 $q\in Q$, $q-1$ 无平方因子, 且所有素因子均在 P 中. 例如, 集合 $P=\{2, 3, 5, 7\}$, $Q=\{2, 3, 7, 11, 31, 43, 71, 211\}$, $210=5\times 42=2\times 3\times 5\times 7$ 可验证满足上述要求.

令 $z = \prod_{p \in P} p$, $\omega = \prod_{q \in Q} q$. 容易看出, 对所有 $q \in Q$, 有 $q-1|z$, 且对所有 $a \in \mathbb{Z}_{\omega}^{*}$, 有 $\mathrm{ord}_{\omega}(a)|z$, 故 $a^{z} \equiv 1(\mathrm{mod}\ \omega)$.

定理 9.7　设 P, Q 满足如上所述的条件, 假设奇数 n 满足

(1) 对所有满足 $q \in Q$ 且 $p|q-1$ 的素数对 (p, q), 下列同余式成立:

$$\tau(\chi_{p,q})^{n^{p-1}-1} \equiv \chi_{p,q}(n)\,(\mathrm{mod}\ n\mathbb{Z}[\xi_p, \xi_q]).$$

(2) 对所有 $p \in P$, 且 $r|n$ 的素数对 (p, r), 下列不等式成立:

$$\nu_p(r^{p-1}-1) \geqslant \nu_p(n^{p-1}-1),$$

则 n 的任一素因子 r 一定属于集合 $\{n^{i}(\mathrm{mod}\ \omega)|\ 0 \leqslant i < z\}$.

证明　令 $R = \mathbb{Z}[\xi_p, \xi_q]$, 设 $e_p = \nu_p(n^{p-1}-1)$, 那么 $n^{p-1} = 1 + a_p p^{e_p}$, $p \nmid a_p$, 且 $r^{p-1} = 1 + b_p(r)p^{e_p}$, 由引理 9.4 知

$$\chi(r) \equiv \tau(\chi)^{r^{p-1}-1}\,(\mathrm{mod}\ rR),$$

于是

$$\chi(r)^{a_p} \equiv \tau(\chi)^{a_p(r^{p-1}-1)} = \tau(\chi)^{b_p(r)(n^{p-1}-1)}\,(\mathrm{mod}\ rR).$$

由引理 9.4 知

$$\tau(\chi)^{n^{p-1}-1} \equiv \chi(n)\,(\mathrm{mod}\ nR) \equiv \chi(n)\,(\mathrm{mod}\ rR),$$

由引理 9.5 得 $\chi(r)^{a_p} = \chi(n)^{b_p(r)}$, 因为 $p \nmid a_p$, 所以 $\chi(r) = \chi(n)^{\ell_p(r)}$, 其中 $\ell_p(r) \equiv a_p^{-1} b_p(r)(\mathrm{mod}\ p)$, 即 $a_p \ell_p(r) = b_p(r)(\mathrm{mod}\ p)$.

取 P 中所有素数为模, 用中国剩余定理知, 存在 $0 \leqslant \ell(r) < z$, 且对所有 $p|z$, 有

$$\ell(r) \equiv -\ell_p(r)\,(\mathrm{mod}\ p).$$

那么$\chi(rn^{\ell(r)}) = 1$, $rn^{\ell(r)} \in \ker \chi = \langle g^{p} \rangle$, g 是 $\mathbb{Z}_q^{*}$ 中某个生成元, p 跑遍 $q-1$ 的任一素因子, 即 $rn^{\ell(r)} \equiv 1(\mathrm{mod} q)$, 故 $rn^{\ell(r)} \equiv 1(\mathrm{mod}\ \omega) \Rightarrow r \equiv n^{z-\ell(r)}(\mathrm{mod}\ \omega)$, 证毕.

注意到, 条件 (2) 的验证需要知道 n 的素因子, 下面的定理解决这一问题.

定理 9.8　令 p, q 是素数, $p|q-1$, 且满足 $\chi_{p,q}(n) \neq 1$ 和 $\tau(\chi_{p,q})^{n^{p-1}-1} \equiv \chi_{p,q}(n)\ (\mathrm{mod}\ n\mathbb{Z}[\xi_p, \xi_q])$, 那么对 n 的任意素因子 r, 有 $\nu_p(r^{p-1}-1) \geqslant \nu_p(n^{p-1}-1)$.

证明　令 $R = \mathbb{Z}[\xi_p, \xi_q]$, 由引理 9.4 知

$$\tau(\chi)^{r^{p-1}-1} \equiv \chi(r)\,(\mathrm{mod}\ rR),$$

所以 $\tau(\chi)$ 在 R/rR 中的阶 $h=\mathrm{ord}(\tau(\chi_{p,q}))\mid p(r^{p-1}-1)$.

另一方面, 由条件知

$$\tau(\chi)^{n^{p-1}-1}\equiv\chi(n)\,(\mathrm{mod}\ nR)\not\equiv 1\,(\mathrm{mod}\ rR),$$

因而 $h|p(n^{p-1}-1)$, $h\nmid n^{p-1}-1$, 故 $p\ |h$. 令 $h=p\cdot h'$, 那么 $h'|(r^{p-1}-1)$, 故 $\nu_p(h')\leqslant\nu_p(r^{p-1}-1)$. 而 $\nu_p(h')=\nu_p(n^{p-1}-1)$, 于是 $\nu_p(r^{p-1}-1)\geqslant\nu_p(n^{p-1}-1)$, 证毕.

现在可以描述分圆环素性检验算法.

算法 分圆环检验 (n).

输入: n

输出: “素数” 或 “合数”

1. 若 n 是一个完全平方数, 则输出 “合数”

   $z\leftarrow 1$

2. $z\leftarrow$ 大于 z 的最小的无平方因子的整数

   (a) [2.1]分解 z 为素因子的乘积 $z=\prod\limits_i p_i$

   2.2 $P\leftarrow\{p_i\}$

   (b) [2.3]$Q\leftarrow\{q\leqslant z+1|\ q素数, q-1|z\}$

   (c) [2.4]$\omega\leftarrow\prod\limits_{q\in Q}q$

   (d) [2.5]若 $\omega>\sqrt{n}$, 执行第 3 步, 否则, 返回第 2 步

3. 若 $n\in P$ 或 $n\in Q$, 则输出 “素数”
4. 若 n 可被 P 或 Q 中的素数整除, 则输出 “合数”
5. 对所有的 $(p,q)\in P\times Q$, 且满足 $p|q-1$,

   若 $\tau(\chi_{p,q})^{n^{p-1}-1}\not\equiv\chi_{p,q}(n)(\mathrm{mod}\ n)$, 则输出 “合数”

6. 对所有的 $p\in P$, 执行

   6.1 $q\leftarrow$ 最小的 mod p 同余 1, 且 $n^{(q-1)/p}\not\equiv 1(\mathrm{mod}\ q)$ 的素数

   6.2 若 $n=q$, 则输出 “素数”

   6.3 若 $q|n$, 则输出 “合数”

   6.4 选择 $\chi_{p,q}$, 若 $\tau(\chi_{p,q})^{n^{p-1}-1}\not\equiv\chi_{p,q}(n)(\mathrm{mod}\ n)$, 则输出 “合数”

7. 从 $i=0$ 到 $z-1$ 执行

   $r_i\leftarrow n^i(\mathrm{mod}\ \omega)$

   若 r_i 是 n 的一个真因子, 则输出 “合数”; 否则输出 “素数”

9.6　基于椭圆曲线的素性检验

Miller-Rabin 检验是一个概率型的素性检验, 利用这个方法, 当输出结果为 “n 是合数” 时, n 一定是合数, 当输出结果为 “n 是素数” 时, 仅以 $1-4^{-T}$ 的概率保证 n 是素数. 9.3 节和 9.4 节中介绍的方法, 则是确定型的素性检验, 当 n 通过这些方法的检验时, n 一定是素数. 但这两种方法依赖于 $n-1$ 或 $n+1$ 的完全或部分分解. 9.5 节介绍的分圆环检验是确定型的, 本节介绍基于椭圆曲线的素性检验, 它也是确定型的.

定理 9.9(Goldwasser-Kiliam)　设 n, r 为大于 3 的整数, 且 $r > (n^{1/4}+1)^2$. 设 A, B, a 和 b 为模 n 整数, 使得 (a,b) 是椭圆曲线

$$E: y^2 = x^3 + Ax + B \pmod n$$

上阶为 r 的点, 那么, 如果 r 是素数, 则 n 是素数.

证明　若 n 不是素数, 则它一定有一个素因子 $p \leqslant \sqrt{n}$, (a,b) 是椭圆曲线

$$E_p: y^2 = x^3 + Ax + B \pmod p$$

上的点. 由于 r 是素数, 所以 (a,b) 在 E_p 上的阶仍是 r, 因而由定理 7.16,

$$r \leqslant |E_p(F_p)| \leqslant p + 1 + 2\sqrt{p} = (\sqrt{p}+1)^2 \leqslant (n^{1/4}+1)^2,$$

与定理中的假设矛盾, 即证.

定理 9.9 将判断 n 是否为素数的问题, 转化为判断 r 是否为素数的问题. 一般可以使 r 比 n 小. 于是反复利用该定理, 得到一串递减的数

$$n = r_0 > r_1 > r_2 > \cdots > r_s, \quad r_i > (r_{i-1}^{1/4}+1)^2 \quad (1 \leqslant i \leqslant s).$$

当 r_i $(1 \leqslant i \leqslant s)$ 是素数时, r_{i-1} 就是素数. 若 r_s 足够小, 可用不超过 $\sqrt{r_s}$ 的所有素数试除 r_s, 判断 r_s 是否为素数. 当 r_s 为素数时就证明了 n 是素数. 这是一个确定型的检验方法.

为了提高上述方法的成功概率, 要求每个 r_i $(0 \leqslant i \leqslant s)$ 都是概率型素数, 即要求它们能通过 Miller-Rabin 检验. 该方法的主要计算量在于对每个 i $(0 \leqslant i \leqslant s)$, 构造 $\mathbb{Z}/r_i\mathbb{Z}$ 上的椭圆曲线 $E_i: y^2 = x^3 + A_i x + B_i$, 使其阶为一个近似素数 kr_{i+1}, 其中 r_{i+1} 为一个满足上述条件的概率型素数, k 是一个光滑数 (即 k 为所有素因子都不超过一个较小的给定上界). 假设 E_i 已构造出来, 任取 E_i 上一点 P, 则 $Q = kP$ 或为 $\mathcal{O}$, 或具有阶 r_{i+1}. 所以在 E_i 上找到阶为 r_{i+1} 的点是不难的.

r_i 是概率型素数, 但假定它是一个素数, 这时可利用复乘的方法构造一条满足上述要求的常规 (即非超奇异) 椭圆曲线 E_i. 以 t 表示 E_i 上的 Frobenius 变换的迹, 令

$$Z = 4r_i - t^2,$$

由定理 7.16 可知 Z 是一个正整数. Z 可表为

$$Z = DY^2,$$

其中 D 是一个无平方因子的正整数. 因而不定方程

$$4r_i = X^2 + DY^2 \tag{9.4}$$

有解. 曲线 E_i 上的点数

$$\#E_i(F_{r_i}) = r_i + 1 - X \tag{9.5}$$

通过选择较小的无平方因子正整数 D, 使方程 (9.4) 有解, 且使 $\#E_i(F_{r_i})$ 为一个近似素数 kr_{r+1}, 其中 r_{i+1} 为符合条件 $r_{i+1} > (r_i^{1/4} + 1)^2$ 的概率型素数, 在 D 选定后, 利用复乘方法可以构造 E_i, 使 $\#E(F_{r_i})$ 为式 (9.5) 中给定的数. 由于篇幅所限, 本书不能介绍复乘方法, 可参阅文献 [21].

第 10 章　大整数因子分解算法

10.1　连分数因子分解算法

设 N 为需要分解因子的正整数, 假如能找到两个整数 A, B, 使

$$A^2 \equiv B^2 \pmod{N}, \tag{10.1}$$

从而 $N|(A+B)(A-B)$. 若 $N \nmid A+B$, $N \nmid A-B$, 则 $(A+B, N)$ 就是 N 的真因子, 从而能分解 N. 当 N 为两个素因子之积时, $N|A+B$ 或 $N|A-B$ 的概率为 1/2 , 若找到 10 个形如式 (10.1) 的同余式, 就有 99.9% 的可能性分解 N.

假设 $p_1 = 2$, $p_2, \cdots, p_k$ 为最小的 k 个素数 (也可以是任意选定的 k 个素数), 首先设法找出一批整数 $\{a_i | 1 \leqslant i \leqslant l\}$, 使 $a_i^2 \equiv b_i \pmod{N}$ $(0 < b_i < N)$, 而每个 b_i 的素因子都在 $p_1, \cdots, p_k$ 之中. 设 $b_i = \prod\limits_{j=1}^{h} p_j^{e_{ij}}$, 将 b_i 对应 $\mathbb{F}_2$ 上的一个 k 维向量 $(c_{i1}, c_{i2}, \cdots, c_{ik})$, 这里当 e_{ij} 为偶数时, $c_{ij} = 0$, e_{ij} 为奇数时, $c_{ij} = 1$, 当某几个向量之和为零时, 它们对应的几个同余式两端相乘, 就可以得到一个形如式 (10.1) 的同余式.

把上述因子分解的方法称为 “同余式的组合方法”, 以下介绍几个具体构造这些同余式的方法, 本节介绍连分数法, 10.5 节介绍数域筛法.

令 $\alpha = \sqrt{N}$, 求 α 的简单连分数展开式, 利用 5.2 节的方法, 取 $a_0 = [\sqrt{N}]$, 令

$$\alpha_1' = \frac{1}{\alpha - [\alpha]}, \quad a_1 = [\alpha_1'];$$

再令

$$\alpha_2' = \frac{1}{\alpha_1' - [\alpha_1']}, \quad a_2 = [\alpha_2'];$$

依此类推, 得到连分数 $[a_0, a_1, a_2, \cdots]$, 令

$$\begin{aligned} &p_{-1} = 1, \quad p_0 = a_0, \quad p_n = a_n p_{n-1} + p_{n-2}, \quad n \geqslant 1, \\ &q_{-1} = 0, \quad p_0 = 1, \quad\ \ q_n = a_n q_{n-1} + q_{n-2}, \quad n \geqslant 1, \end{aligned}$$

则 p_n/q_n 为 α 的最佳渐近分数.

定理 10.1　当 $n \geqslant 0$ 时,

$$p_n^2 \equiv (-1)^{n-1} Q_n \pmod{N}, \quad 且 0 < Q_n < 2\sqrt{N}.$$

证明 当 $n=0$ 时, 取 $Q_0=N-[\sqrt{N}]^2$, 则 $p_0^2\equiv -Q_0(\bmod N)$ 且

$$Q_0=N-(\sqrt{N}-\{\sqrt{N}\})^2=\{\sqrt{N}\}(2\sqrt{N}-\{\sqrt{N}\})<2\sqrt{N}.$$

设 $n\geqslant 1$, 由定理 5.4 的证明, 则有

$$p_n-\alpha q_n=\frac{(-1)^{n-1}}{\alpha'_{n+1}q_n+q_{n-1}},$$

以及

$$\alpha=\frac{\alpha'_{n+1}p_n+p_{n-1}}{\alpha'_{n+1}q_n+q_{n-1}},$$

因而

$$\begin{aligned}
p_n^2&\equiv\frac{2\alpha q_n(-1)^{n-1}}{\alpha'_{n+1}q_n+q_{n-1}}+\frac{1}{(\alpha'_{n+1}q_n+q_{n-1})^2}(\bmod N)\\
&\equiv(-1)^{n-1}\cdot 2\alpha\left(\frac{q_n}{\alpha'_{n+1}q_n+q_{n-1}}+\frac{(-1)^{n-1}}{2(\alpha'_{n+1}p_n+p_{n-1})(\alpha'_{n+1}q_n+q_{n-1})}\right)(\bmod N)\\
&\equiv(-1)^{n-1}\cdot 2\alpha\left(\frac{2\alpha'_{n+1}p_nq_n+2p_{n-1}q_n+(-1)^{n-1}}{2(\alpha'_{n+1}p_n+p_{n-1})(\alpha'_{n+1}q_n+q_{n-1})}\right)(\bmod N)\\
&\equiv(-1)^{n-1}\cdot 2\alpha\left(\frac{2\alpha'_{n+1}p_nq_n+p_nq_{n-1}+p_{n-1}q_n}{2(\alpha'_{n+1}p_n+p_{n-1})(\alpha'_{n+1}q_n+q_{n-1})}\right)(\bmod N).
\end{aligned}$$

由于 $\alpha'_{n+1}\geqslant 1$, 上述分数的分子小于分母, 故证得 $0<Q_n<2\sqrt{N}$.

由定理 10.1, 利用 $\sqrt{N}$ 的连分数展开, 可以得到一批同余式

$$p_n^2\equiv(-1)^{n-1}Q_n(\bmod N).$$

由于 $0<Q_n<2\sqrt{N}$, 所以 Q_n 比较小, 它的所有素因子很可能在预先选定的 k 个素数 $p_1,\cdots,p_k$ 之内, 符号 $(-1)^{n-1}$ 也可把它作为一个素因子处理. 利用上述 "同余式的组合方法", 可以得出一批同余式 (10.1). 把 $p_1,\cdots,p_k$ 这组素数称为分解基, 可以证明当 $p|Q_n$ 时, 一定有 $\left(\dfrac{N}{p}\right)=1$, 所以应选取适合 $\left(\dfrac{N}{p}\right)=1$ 的素数组成分解基. 在计算时, 用分解基中的素数去试除 Q_n, 设法找出素因子全部在分解基中的那些 Q_n, 这是连分数因子分解算法中最费时间的一部分.

令 $L(N)=\exp(\sqrt{\log N\log\log N})$, 可以证明上述标准的连分数因子分解算法的计算量 (当 $N\to\infty$ 时) 为 $L(N)^{\sqrt{2}+o(1)}$($o(1)$ 表示一个无穷小量, 当 $N\to\infty$ 时它趋于零). 将上述方法作适当变化后, 该渐近计算量可改进为 $L(N)^{1+O(1)}$.

10.2　二 次 筛 法

令 $Q(x)=([\sqrt{N}]+x)^2-N$, 因而 $Q(x)\equiv([\sqrt{N}]+x)^2(\bmod N)$. 当 $A\neq 0$ 时, $0<Q(A)<2\sqrt{N}|A|+A^2$, 所以当 $|A|\leqslant N^{1/4}$ 时, $Q(A)$ 近似于 $2\sqrt{N}|A|$，其值较小, 它的所有素因子很可能在分解基 $p_1<\cdots<p_k$ 内. 但可以不用像使用连分数方法时, 依次用分解基内的素数去试除 $Q(A)$, 以确定它的所有素因子是否都在分解基内.

设分解基内的素数都适合 $\left(\dfrac{N}{p}\right)=1$, 若 p 为分解基内的一个素数, 同余方程

$$Q(x)\equiv 0\,(\bmod\ p)$$

有两个解 A_1, A_2. 在区间 $-M<x<M$(M 预先选定) 内, 将所有的 $Q(x)$ 计算排列起来. 当 $x\equiv A_1$ 或 $x\equiv A_2(\bmod\ p)$ 时, $Q(x)$ 能被 p 除尽, 因而可以筛出这些 x, 并计算 $Q(x)/p$, 将它代替 $Q(x)$ 储存. 对分解基内的每个素数, 重复上述过程. 最后, 若对某个 x, 对应它所存储的 $Q(x)\leqslant p_k$, 这样的 x 就是所要筛选的. 在这个筛选过程中, 并不用分解基中的素数对 $Q(x)$ 进行试除, 做很多除法, 而是仅当知道 $Q(x)$ 是 p 的倍数时才做除法, 这节省了计算时间.

在以上的筛选过程中, 没有考虑 $Q(x)$ 能被分解基内的素数的幂整除的情况. 如果要考虑素数幂, 在计算 $Q(x)/p$ 后, 可以再用 p 去试除它, 或者对应某些素数的幂 p^k, 利用同余式

$$Q(x)\equiv 0\,(\bmod\ p^k)$$

的解进行筛选.

当 x 增加时, $Q(x)$ 会迅速增加, 因而它的素因子很可能会超出了分解基的范围, 这是上述方法的一个缺点. 可以在适当的时候, 选用另一个二次多项式, 以得到较小的多项式的值, 这称为重多项式二次筛法. 下面介绍两个变换二项式的方法.

在利用 $Q(x)$ 进行筛法的过程中, 假如遇到了一个 A_0, 其对应的 $Q(A_0)$ 有一个大素因子 q, q 不属于分解基, 但 $Q(A_0)$ 的其他素因子都在分解基内. 定义 $Q_q(x)=Q(A_0+qx)$, 易见 $q|Q_q(x)$, $Q_q(x)/q\approx 2\sqrt{N}|x|$. $Q_q(0)=Q(A_0)$ 是已有的数, 而当 $x\neq 0$ 时, $Q_q(x)/q$ 是一批新的数, 以 $Q_q(x)$ 代替 $Q(x)$, 仍用同样的分解基进行筛法. 不过这时知道每个 $Q_q(x)$ 都有一个素因子 q, 而

$$Q_q(x)\equiv([\sqrt{N}]+A_0+qx)^2\,(\bmod\ N).$$

这个方法是 Davis 和 Hddridge[13] 提出来的.

Montgomery[35] 提出另一个方法. 令 $F(x)=ax^2+2bx+c$, 若 $N|b^2-ac$, 则

$$aF(x)=(ax+b)^2-(b^2-ac)\equiv(ax+b)^2\,(\bmod\ N),$$

即 $aF(x)$ 模 N 是平方剩余, 当 $-M \leqslant x \leqslant M$ 时, 希望 $|F(x)|$ 较小. 为此, 取 a 为素数, $a \approx \dfrac{\sqrt{2N}}{M}$, a 适合 $\left(\dfrac{N}{a}\right) = 1$. 设 b 适合 $b^2 \equiv a(\mathrm{mod}\ N)$, 令 $c = \dfrac{b^2 - N}{a}$, 因而 $b^2 - ac = N$. 取适合上述条件不同的 a, 就可得到不同的二项式, 而 $|F(x)|$ 的值比 $Q(x)$ 的值 (在区间 $-M \leqslant x \leqslant M$ 内) 略小.

经过适当改进后, 二次筛法的计算复杂度也可达到 $L(N)^{1+o(1)}(N \to \infty)$.

10.3 Pollard 的 $p-1$ 因子分解算法

本节介绍另一种类型的因子分解算法.

设 p 为奇素数, 由 Fermat 小定理 2.6 可知

$$2^{p-1} \equiv 1\,(\mathrm{mod}\ p).$$

若 m 为任一整数, $p-1|m$, 则有 $2^m \equiv 1(\mathrm{mod}\ p)$.

设 N 为要分解的整数, p 为 N 的一个奇素因子, p 是未知的. 若 $p-1|k!$, 则 $p|(2^{k!}-1, N)$, 计算 $(2^{i!}-1, N)$ 就可将 N 分解. 我们可以依次计算 $(2^{i!}-1, N), i = 1, 2, \cdots$, 当 i 足够大时, 就可能得到 N 的分解.

我们也可以用 $p_1 p_2 \cdots p_k$(最小的 k 个素数之积) 代替 $k!$, 当 $p-1$ 的素因子都在 $p_1, \cdots, p_k$ 之中, 且没有重因子时, 就可能成功分解 N. $p-1$ 有重因子的情况是很少发生的.

Pollard 的 $p-1$ 算法是利用了群 $(\mathbb{Z}/p\mathbb{Z})^*$, 也可以利用其他的群. 椭圆曲线因子分解算法就是这种类型的一个算法.

10.4 椭圆曲线因子分解算法

10.3 节介绍的 Pollard 的 $p-1$ 因子分解算法基于乘法群 $(\mathbb{Z}/p\mathbb{Z})^*$. 也可以利用其他的群. 本节将介绍的椭圆曲线因子分解算法基于 F_p 上的椭圆曲线上的点所形成的群 $E(F_p)$. 由于 F_p 上的椭圆曲线可以有很多不同的选择, 这可以增加分解成功的可能性.

设 N 为要分解的合数, 将利用环 $\mathbb{Z}/N\mathbb{Z}$ 上的椭圆曲线, 但并不打算严格地引入环上椭圆曲线的概念 (关于这方面的内容可以参阅文献 [23]). 实际上仅需要利用其上的一个子集, 具有有限域上椭圆曲线的概念就可以了.

设 N 与 $2, 3$ 互素, $a, b \in \mathbb{Z}/N\mathbb{Z}$ 且 $4a^3 + 27b^2$ 与 N 互素, 方程

$$y^2 = x^3 + ax + b$$

定义 $\mathbb{Z}/N\mathbb{Z}$ 上的椭圆曲线 $E_{a,b}$, 取 $E_{a,b}$ 上的子集

$$V_N = \{(x,y,1)|x,y\in\mathbb{Z}/N\mathbb{Z}\}\cup\{\mathcal{O}\},$$

其中 $\mathcal{O}=(0,1,0)$. 在 V_N 上定义 "加法运算".

取 $P,Q\in V_N$, 以 R 表示 P 与 Q 之和. 若 $P=\mathcal{O}$, 则 $R=Q$; 若 $Q=\mathcal{O}$, 则 $R=P$. 当 $P\neq\mathcal{O},Q\neq\mathcal{O}$ 时, 记 $P=(x_1,y_1,1)$, $Q=(x_2,y_2,1)$, 计算 $\gcd(x_1-x_2,N)$, 若它是 N 的真因子, 计算停止; 若 $\gcd(x_1-x_2,N)=1$, 计算

$$\lambda=(y_1-y_2)(x_1-x_2)^{-1},\quad x_3=\lambda^2-x_1-x_2,\quad y_3=\lambda(x_1-x_3)-y_1,$$

这时 $R=(x_3,y_3,1)$; 若 $\gcd(x_1-x_2,N)=N$, 即 $x_1=x_2$, 计算 $\gcd(y_1+y_2,N)$, 若它是 N 的一个真因子, 计算停止; 若 $\gcd(y_1+y_2,N)=N$, 即 $y_1=-y_2$, 则 $R=\mathcal{O}$; 若 $\gcd(y_1+y_2,N)=1$, 计算

$$\lambda=(3x_1^2+a)(y_1+y_2)^{-1},\quad x_3=\lambda^2-x_1-x_2,\quad y_3=\lambda(x_1-x_3)-y_1,$$

这时 $R=(x_3,y_3,1)$. 以上定义的 "加法" 运算, 计算的结果或是得到 N 的一个真因子, 或是得到 $R=P+Q\in V_N$.

N 给定后, 任取 $(a,\alpha,\beta)\in(\mathbb{Z}/N\mathbb{Z})^3$, 令 $b=\beta^2-\alpha^3-a\alpha(\bmod N)$, 如果 $4a^3+27b^2$ 与 N 互素, 则得到 $\mathbb{Z}/N\mathbb{Z}$ 上的椭圆曲线 $E_{a,b}$(否则另取一组 (a,α,β) 再试). 令 $P=(\alpha,\beta,1)$, P 为 $E_{a,b}$ 上的一点, 取一大整数 k(例如, $k=i!$, 或用其他取法), 计算 kP. 由上述 V_N 上 "加法" 的定义, 可能有两个计算结果, 一是在计算过程中找到 N 的一个真因子, 这时分解 N 成功; 另一结果是算得 $R=kP\in V_N$, 这时分解 N 没有成功, 可以另取一组 (a,α,β), 重复上述计算. 这就是椭圆曲线因子分解算法, 它是一个概率型算法.

下面给出一个能使该算法分解成功的充分条件. 设 N 至少有两个素因子 p 和 q, p 为 N 的最小素因子. 记 $P=(\alpha,\beta,1)$, $P_p=(\alpha(\bmod p),\beta(\bmod p),1)$, $\overline{a}=a(\bmod p)$, $\overline{b}=b(\bmod p)$, $\widehat{a}=a(\bmod q)$, $\widehat{b}=b(\bmod q)$, 假设下述条件成立:

(1) $4\overline{a}^3+27\overline{b}^2\neq 0(\bmod p)$, $4\widehat{a}^3+27\widehat{b}^2\neq 0(\bmod q)$;

(2) $|E_{\overline{a},\overline{b}}(F_p)|$ 是 k 的因子;

(3) P_p 在 $E_{\overline{a},\overline{b}}(F_p)$ 中的阶 $\mathrm{ord}(P_p)$ 的最大素因子不是 $|E_{\widehat{a},\widehat{b}}(F_q)|$ 的因子,

则计算 kP 一定能得到 N 的真因子.

利用反证法, 假设计算 kP 得到 V_N 中的一个点, 则对任意 $0<k'<k$, $k'P$ 也是 V_N 中的一个点. 设 $\mathrm{ord}(P_p)$ 的最大素因子为 l, 由于 $\mathrm{ord}(P_p)\,\big|\,|E_{\overline{a},\overline{b}}(F_p)|\,\big|\,k$, 取 $k_0=(\mathrm{ord}\ (P_p))/l$, 所以

$$k_0P_p\neq\mathcal{O}_p,\quad k_0lP_p=\mathcal{O}_p,$$

$\mathcal{O}_p$ 为 $E_{\overline{a},\overline{b}}(F_p)$ 上的无穷远点. 对于 V_N 中的任一点 R, 当且仅当 $R=\mathcal{O}$ 时, $R_p=\mathcal{O}_p$. 可见 $k_0lP=\mathcal{O}$, 这时 $k_0lP_q=\mathcal{O}_q$. 由于条件 (3), 可知 $k_0P_q=\mathcal{O}_q$, 从而 $k_0P=\mathcal{O}$, 这与上述 $k_0P_p\neq\mathcal{O}_p$ 矛盾.

文献[28]在某些假设成立的前提下证明了椭圆曲线因子分解的计算复杂度为

$$\mathrm{e}^{(1+o(1))\sqrt{\log N\cdot\log\log N}},\quad N\to\infty.$$

这个证明所需的椭圆曲线知识超出了本书的范围, 这里不再叙述, 当 N 的第二大素因子接近 $\sqrt{N}$ 时, 这个方法所需计算量最大. 有一些其他的因子分解算法, 如连分数因子分解算法和二次筛法, 也具有上述相同的计算复杂度. 当 N 为两个大小接近的素因子乘积时, 利用二次筛法最为有效. 但椭圆曲线因子分解算法也是一个在很多情况下需要利用的重要的因子分解算法.

10.5 数域筛法

数域筛法是目前最有效的大数分解算法, 这种算法的期望时间复杂度为

$$L_n\left(\frac{1}{3},\ \left(\frac{64}{9}\right)^{\frac{1}{3}+o(1)}\right),$$

其中 n 是待分解的大整数, $L_n(a,b)=\exp\left(b(\log n)^a(\log n)^{1-a}\right)$. 在 1990 年, Lenstra 等用特殊数域筛法成功地分解了第 9 个 Fermat 数 $F_9=2^{512}+1$, 这是一个 155 位的整数, 由于 F_9 的一个 7 位素因子 P_7 在分解前就知道, 实际上他们将 F_9/P_7 这个 148 位的整数分解成一个 49 位整数和一个 99 位素数的乘积. 而用其他的分解算法都没成功. 至今, 用一般数域筛法因子分解的最好记录是 2009 年 12 月分解了 RSA-768, 此前其他算法都没能成功分解. RSA-768 是两个十进制 116 位 (384 比特) 的素数之积.

数域筛法和连分数分解算法、二次筛法一样, 都属于同余式的组合方法范畴, 关键的不同之处在于收集关系的方式不同. 顾名思义, 数域筛法要涉及代数数域的理论. 它的思路大致是: 选择一个代数整数 $\theta\notin\mathbb{Q}$, 由此产生代数数域 $K=\mathbb{Q}(\theta)$, 令 $f(x)\in\mathbb{Z}[x]$ 是 θ 的极小多项式, 假若知道一个整数 m 使 $f(m)=kn$, 那么就可定义从 K 的阶 $\mathbb{Z}[\theta]$ 到剩余类环 $\mathbb{Z}_n$ 之间的环同态

$$\varphi\left(\sum_{i=0}^{n-1}a_i\theta^i\right)=\sum_{i=0}^{n-1}a_im^i\ (\mathrm{mod}\ n).$$

我们希望能找到一个有限集合

$$S\subseteq\{(a,b)\in\mathbb{Z}\times\mathbb{Z}\mid\ \gcd(a,b)=1\},$$

同时满足

$$\prod_{(a,b)\in S}(a+bm)\text{是 }\mathbb{Z}\text{ 中平方元,} \tag{10.2}$$

$$\prod_{(a,b)\in S}(a+b\theta)\text{是 }\mathbb{Z}[\theta]\text{ 中平方元,} \tag{10.3}$$

令 x 是式 (10.2) 的平方根, α 是式 (10.3) 的平方根, 那么

$$\varphi(\alpha^2) = x^2 \pmod{n}.$$

令 $y=\varphi(\alpha)$, 便得同余式

$$y^2 \equiv x^2 \pmod{n}.$$

下面只需计算 $\gcd(x-y,n)$, 期望找到 n 的一个因子.

上述整个过程中有几个假设, 如何实现这些假设是数域筛法可用性的关键:

(1) 多项式 f 和整数 m 如何构造?

(2) 集合 S 如何构造?

(3) 元素 $\alpha\in\mathbb{Z}[\theta]$ 如何寻找, 使 α^2 为式 (10.3)(即 $\mathbb{Z}[\theta]$ 中求平方根的算法)?

(4) 每一步所花费多少时间?

1. 寻找多项式

首一整系数多项式 $f(x)$ 和整数 m 的选择要满足

$$f(m)\equiv 0 \pmod{n}.$$

首先选定 f 的次数为 $d>1$, 为使整个算法尽可能简单, d 一般较小. 一种最简单的方法是取 $m=[n^{\frac{1}{d}}]$, 然后将 n 写成 m 进制形式

$$n = c_d m^d + \cdots + c_1 m + c_0, \quad 0 \leqslant c_i < m.$$

令 $f(x)=c_d x^d+\cdots+c_1 x+c_0$, 即达到要求.

引理 10.1　若 $d>1$ 且 $n\geqslant 2^{d^2}$, 则 $c_d=1$, $c_{d-1}\leqslant d$.

证明　因为 $m=[n^{\frac{1}{d}}]$, 所以 $m<n^{\frac{1}{d}}\leqslant m+1$, 于是

$$m^d < n < (m+1)^d = m^d + \sum_{i=1}^{d-1}\binom{d}{i}m^i + 1,$$

而对 $1\leqslant i\leqslant d-1$, 有二次式系数不等式 $\binom{d}{i}\leqslant 2^d-2\leqslant n^{\frac{1}{d}}-2\leqslant m-1$, 因此上述右边的等式事实上是 $(m+1)^d$ 的 m 进制表示, 故 $c_d=1$, $c_{d-1}\leqslant d$, 证毕.

假若 $f(x)$ 可约, 即 $f(x) = g(x) \cdot h(x)$, $1 \leqslant \deg g(x) < d$, 那么

$$n = g(m)h(m)$$

给出 n 的一个非平凡的分解, 这一步完全由整系数多项式的分解算法来完成. 若用第 13 章中涉及 LLL 算法的分解算法, 那么 n 分解的复杂度为 $(\log n)^{o(1)}$. 因此以后均在下面的条件下讨论:

(1) $n > 2^{d^2}$;

(2) $m = [n^{\frac{1}{d}}]$;

(3) $f(x) = \sum\limits_{i=0}^{d} c_i x^i \in \mathbb{Z}[x]$ 不可约, 其中 $n = \sum\limits_{i=0}^{d} c_i m^i, 0 \leqslant c_i < m$.

引理 10.2 $|\Delta(f)| < d^{2d} n^{2-\frac{3}{d}}$.

证明 由习题 6.2 可知, $|\Delta(f)| = |\mathrm{res}(f, f')| = |\det M|$, 其中

$$M = \begin{pmatrix} 1 & c_{d-1} & \cdots & \cdots & & c_1 & c_0 & & \\ & 1 & c_{d-1} & \cdots & & & & & \\ & & \ddots & & & & & & \\ & & & & 1 & c_{d-1} & \cdots & \cdots & c_0 \\ d & (d-1)c_{d-1} & \cdots & & & c_1 & \cdots & \cdots & \\ & d & \cdots & & & \cdots & \cdots & \cdots & \\ & & \ddots & & & & & & \\ & & & & & d & (d-1)c_{d-1} & \cdots & c_1 \end{pmatrix}$$

用 d 除 M 的后 d 行后再用 m 除后 $2d-3$ 列, 最后用 c_{d-1} 乘第一列去减第二列得矩阵

$$M' = \begin{pmatrix} 1 & 0 & \frac{c_{d-2}}{m} & \cdots & & \frac{c_0}{m} & & \\ & 1 & \frac{c_{d-1}}{m} & \cdots & & \frac{c_1}{m} & \frac{c_0}{m} & \\ & & \ddots & & & & & \\ & & & & 1 & \frac{c_{d-1}}{m} & \cdots & & \frac{c_0}{m} \\ 1 & -\frac{c_{d-1}}{d} & \frac{(d-2)c_{d-2}}{md} & \cdots & & \frac{c_1}{md} & & & \\ & 1 & \cdots & \cdots & & & \cdots & & \\ & & \ddots & & & & & & \\ & & & & & 1 & \frac{(d-1)c_{d-1}}{md} & \cdots & \frac{c_1}{md} \end{pmatrix}$$

因此 $\det M = d^d m^{2d-3} \det M'$. 注意到, 矩阵 M' 中每一个元素的绝对值均 $\leqslant 1$, 前 $d-1$ 行向量的欧几里得长度 $\leqslant (d+1)^{\frac{1}{2}}$, 后 d 行向量的欧几里得长度 $\leqslant d^{\frac{1}{2}}$, 由引理 13.2 的 Hadamard 不等式可知

$$\det M' \leqslant \big(d+1\big)^{\frac{d-1}{2}} d^{\frac{d}{2}},$$

故

$$\det M \leqslant d^d m^{2d-3}\big(d+1\big)^{\frac{d-1}{2}} d^{\frac{d}{2}} \leqslant d^{d+\frac{d}{2}}(d+1)^{\frac{d-1}{2}} n^{2-\frac{3}{d}} < d^{2d} n^{2-\frac{3}{d}},$$

证毕.

2. 筛法

首先寻找有限集合 T_1, 使得 T_1 中的每个元素 (a,b) 所确定的 $a+bm$ 都是 y-光滑的.

令 u 为一个事先约定好的相对于 n 较小的正整数, 首先用筛法构造集合

$$U = \left\{(a,b) \in \mathbb{Z}^2 \middle|\ \gcd(a,b)=1, |a| \leqslant u, 0 < b < u\right\}.$$

然后选择一个和 n 有关的参数 $y = y(n)$, 再用筛法获得一个 U 的子集合

$$T_1 = \left\{(a,b) \in U \middle|\ a+bm \text{ 是 } y\text{-光滑的}\right\}.$$

具体地, 对每个 $b(0<b<u)$, 它的分解是容易知道的. 取 b 的每个素因子, 用试除法去筛 a, 筛剩下的对 (a,b) 构成集合 U, 然后固定 b, 对每个 $(a,b)\in U$, 赋予一个初始值 $S_a = 0$, 取每个素数 $p \leqslant y$, 对那些满足 $a \equiv -bm \pmod p$ 的对 (a,b), 令 $S_a + \log p \to S_a$, 当 p 取完后, 对那些逼近 $\log|a+bm|$ 的 S_a, 对应的 $a+bm$ 就是 y-光滑的. 这样 T_1 就构造好了.

定义 $\alpha \in \mathbb{Z}[\theta]$ 是 y-光滑的, 若 $N(\alpha) \in \mathbb{Z}$ 是 y-光滑的. 已知 $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$, 容易推得

$$N(a+b\theta) = a^d - c_{d-1}a^{d-1}b + \cdots + (-1)^d c_0 b^d = F(a,b),$$

其中 $F(x,y) = (-y)^d f(-x/y)$. 再利用和上述相类似的筛法获得集合

$$T_2 = \left\{(a\ b) \in U \middle|\ a+b\theta \text{ 是 } y\text{-光滑的}\right\}.$$

这样便用筛法构造了集合 $T = T_1 \cap T_2$, 对任意 $(a,b)\in T$, $a+bm$, $F(a,b)$ 均是 y-光滑的. 在实际中, 为了能找到更多的关系, 在对 $a+bm$, $F(a,b)$ 同时筛的过程中允许 $a+bm$, $F(a,b)$ 有且只有大于 y 的素因子[31]. 还有一种称作格筛的算法去构造集合 T, 用一些特殊的格去筛 T 中的对, 格筛比上述筛法 (称为线筛) 的效率要高[44].

下面的目的是寻找一个有限集 $S \subseteq T$ 使得式 (10.2) 和式 (10.3) 均成立. 显然要把注意力放在式 (10.3) 上, 即

$$\prod_{(a,b)\in S}(a+b\theta)\text{是 } \mathbb{Z}[\theta] \text{ 中的平方元.}$$

事实上, 可以放松条件, 只需存在 $r \in K$, 使得

$$\prod_{(a,b)\in S}(a+b\theta) = r^2.$$

此时, r 一定在 O_K 中, 由引理 6.3 知 $rf'(\theta) \in \mathbb{Z}[\theta]$, 因此

$$f'(\theta)^2 \prod_{(a,b)\in S}(a+b\theta)\text{便是 } \mathbb{Z}[\theta] \text{ 中的平方元.}$$

又因为 $1 < f'(m) < n$, 不妨设 $\gcd(f'(m), n) = 1$, 否则便给出了 n 的一个真因子, 这样, 用 $f'(m)^2 \prod\limits_{(a,b)\in S}(a+bm)$ 代换式 (10.2) 不会影响对 n 的分解.

首先考虑 $\mathbb{Z}[\theta]$ 中哪些素理想包含 $a+b\theta$.

引理 10.3 $\mathbb{Z}[\theta]$ 中的一次素理想 $\wp$, 一定有形式 $(p, \theta-r) = p\cdot\mathbb{Z}[\theta] + (\theta-r)\mathbb{Z}[\theta]$, 其中 p 是某个素数, r 为满足 $f(r) \equiv 0 (\text{mod } p)$ 的整数.

证明 因为 $\deg\wp = 1$, 即 $\dfrac{\mathbb{Z}[\theta]}{\wp} \cong F_p$, 所以存在一个满同态 $\varphi : \mathbb{Z}[\theta] \to F_p$, 使得 $\ker\varphi = \wp$.

设 $r = \varphi(\theta)$, 则 $f(r) = f(\varphi(\theta)) = \varphi(f(\theta)) \equiv 0 (\text{mod } p)$. 断言 $\wp = (p, \theta-r)$, 显然 $(p, \theta-r) \subseteq \wp$, 反之, 对任意 $\alpha \in \wp$, φ 作用 $\alpha = \sum\limits_{i=0}^{d-1} a_i\theta^i$, 可知 $0 \equiv \sum\limits_{i=0}^{d-1} a_i r^i \pmod p$. 于是

$$\alpha = \sum_{i=0}^{d-1} a_i\theta^i - \sum_{i=0}^{d-1} a_i r^i = (\theta-r)(d(\theta)) \pmod p,$$

其中 $d(\theta) \in \mathbb{Z}[\theta]$, 故 $\alpha \in (p, \theta-r)$, 证毕.

上述引理的逆命题显然也是成立的, 以后令 $R(p) = \{r \in F_p | \ f(r) \equiv 0 (\text{mod } p)\}$, 这样, $\mathbb{Z}[\theta]$ 的一次素理想 $\wp$ 便和数对 $(p, r)(r \in R(p))$ 一一对应.

引理 10.4 设 a, b 是互素的整数, $\wp$ 是 $\mathbb{Z}[\theta]$ 的素理想, 若 $a+b\theta \in \wp$, 那么 $\deg\wp = 1$.

证明 设 $\wp \cap \mathbb{Z} = (p)$, 因为 $a+b\theta \in \wp$, 则 $p \nmid b$, 否则 $a \in \mathbb{Z} \cap \wp = (p)$, 这和 $\gcd(a, b) = 1$ 矛盾. 取 c 使得 $bc \equiv 1 (\text{mod } p)$, 那么 $\theta = -ca (\text{mod } \wp)$, 故 $\mathbb{Z}[\theta]/\wp \cong F_p$, 即 $\deg\wp = 1$, 证毕.

由于 $N(a+b\theta)$ 是个整数, 现将其写成素数的乘积, 有形式

$$N(a+b\theta)=\pm\prod_{p}p^{\nu_p(N(a+b\theta))},$$

p 跑遍所有的素数.

引理 10.5　设 a,b 为一对互素的整数, p 是素数, 则 $\nu_p(N(a+b\theta))>0$ 当且仅当存在 $r\in R(p)$ 使得 $a+b\theta\in\wp=(p,\theta-r)$.

证明　$(\Longleftarrow)$ 令 $A=\mathbb{Z}[\theta]$, 因为 $(a+b\theta)A\subseteq\wp\subseteq A$, 那么

$$p=N(\wp)=|A/\wp|\ \big|\ |A/(a+b\theta)A|=|N(a+b\theta)|,$$

故 $\nu_p(N(a+b\theta))>0$.

$(\Longrightarrow)$ 因为 $\nu_p(N(a+b\theta))>0$, 故

$$N(a+b\theta)=a^d-c_{d-1}a^{d-1}b+\cdots+(-1)^d a_0 b^d\equiv 0\,(\mathrm{mod}\ p),$$

直接推得 $p\nmid b$, 否则和 $\gcd(a,b)=1$ 矛盾, 令 $r=-ab^{-1}(\mathrm{mod}\ p)$, 在上面的同余式两边同乘 b^{-d} 得

$$f(r)\equiv 0\,(\mathrm{mod}\ p),$$

故 $\wp\triangleq(p,\theta-r)$ 是一次素理想. 而 $a+b\theta=b(\theta-r)(\mathrm{mod}\ p)\ \in\wp$, 证毕.

对任意素数 p, $r\in R(p)$, 定义符号

$$e_{p,r}(a+b\theta)=\begin{cases}\nu_p(N(a+b\theta)), & a+br\equiv 0\,(\mathrm{mod}\ p),\\ 0, & \text{否则},\end{cases}$$

这样可表示

$$N(a+b\theta)=\pm\prod_{p,r}p^{e_{p,r}(a+b\theta)}.$$

对任一非零素理想 $\wp$, 由 6.1 节知, 存在 $\ell_\wp$ 是 $K^*\to\mathbb{Z}$ 的群同态, 且 $|N(x)|=\prod\limits_{\wp}N(\wp)^{\ell_\wp(x)}$. 特别地, 取 $x=a+b\theta$ 时, 和上式比较, 可直接得如下推论.

推论 10.1　a,b 是互素的整数, $\wp$ 是 $\mathbb{Z}[\theta]$ 的一个素理想, 那么

$$\ell_\wp(a+b\theta)=\begin{cases}e_{p,r}(a+b\theta), & \wp=(p,\theta-r)\text{是一次素理想},\\ 0, & \text{否则}.\end{cases}$$

引理 10.6　令 $S\subseteq\{(a,b)\in\mathbb{Z}\times\mathbb{Z}|\ (a,b)=1\}$ 是有限集, 且

$$\prod_{(a,b)\in S}(a+b\theta)=h^2\ ,\quad h\in K,$$

那么, 对任意素数 p, 以及 $r \in R(p)$ 有

$$\sum_{(a,b)\in S} e_{p,r}(a+b\theta) \equiv 0 \pmod 2. \tag{10.4}$$

证明 设 $\wp = (p, \theta - r)$ 是 $\mathbb{Z}[\theta]$ 的一次素理想, 那么

$$\begin{aligned}\sum_{(a,b)\in S} e_{p,r}(a+b\theta) &= \sum_{(a,b)\in S} \ell_\wp(a+b\theta) \\ &= \ell_\wp\left(\prod_{(a,b)\in S}(a+b\theta)\right) \\ &= \ell_\wp(h^2) = 2\ell_\wp(h) \equiv 0 \pmod 2,\end{aligned}$$

证毕.

式 (10.4) 给出了 $\prod\limits_{(a,b)\in S}(a+b\theta)$ 是平方元的必要条件, 但不是充分条件. 如对不包含 -1 的平方根的数域 K, 取 $S = \{(-1,0)\}$, 便给出了一个反例.

可以用解 F_2 上线性方程组的算法, 求得 T 的一子集合 $S \subseteq T$, 使得

$$\sum_{(a,b)\in S} \ell_\wp(a+b\theta) \equiv 0 \pmod 2,$$

即

$$\ell_\wp\left(\prod_{(a,b)\in S}(a+b\theta)\right) \equiv 0 \pmod 2,$$

其中 $\wp$ 是一次素理想, 且 $N(\wp) \leqslant y$, 要注意的是, $\prod\limits_{(a,b)\in S}(a+b\theta)$ 不一定是 K 中的平方元. 为了刻画它和平方元之间有多大距离, 构造集合

$$V = \left\{\alpha \in K^* \middle|\, \ell_\wp(\alpha) \equiv 0 \pmod 2,\ \wp\text{跑遍 } \mathbb{Z}[\theta] \text{ 中任一素理想}\right\}.$$

因为 $\ell_\wp$ 是群同态, 所以 $K^{*^2} \subseteq V$, 将商群 V/K^{*^2} 很自然看成 F_2 上的向量空间, 它的维数反映了 V 和 K^{*^2} 之间的区别大小.

定理 10.2 令 $m, f, d \geqslant 2, n > d^{2d^2}$ 同前一样, 那么

$$\dim_{F_2} V/K^{*^2} < \log n / \log 2,$$

即 $[V : K^{*^2}] < n$.

证明　令 $W=\{r\in K^*|\ rO_K=\mathfrak{a}^2,\mathfrak{a}\text{是分式理想}\}$, 由引理 6.13 知 $V\supseteq W$, $[V:W]\leqslant[O_K:\mathbb{Z}[\theta]]$. 令 O_K^* 是 O_K 的所有乘法可逆元构成的集合, $Y=O_K^*\cdot {K^*}^2$, 于是有子群链

$$V\supseteq W\supseteq Y\supseteq {K^*}^2.$$

考虑群同态

$$\begin{aligned}\varphi:W&\longrightarrow Cl(O_K)\\ r&\longmapsto\overline{\mathfrak{a}},\end{aligned}$$

其中 $rO_K=\mathfrak{a}^2$, 显然 $\ker\varphi=Y$. 故

$$[W:Y]\leqslant|Cl(O_K)|=h(K).$$

而 $Y/{K^*}^2$ 显然同构于 $O_K^*/{O_K^*}^2$, 且由 Dirichlet 单位定理 (定理 6.8) 知, $\dim_{F_2}O_K^*/{O_K^*}^2=r_1+r_2$, 故

$$[Y:{K^*}^2]=2^{r_1+r_2}=2^{d-r_2},$$

综合上述得

$$[V:{K^*}^2]\leqslant[O_K:\mathbb{Z}[\theta]]\cdot h(K)\cdot 2^{d-r_2}.$$

令 Δ_K 为 K 的判别式, 由定理 6.6 知

$$h(K)\leqslant M\cdot\frac{(d-1+\log M)^{d-1}}{(d-1)!},$$

其中 $M=(d!/d^d)(4/\pi)^{r_2}\sqrt{|\Delta_K|}$ 是 K 的 Minkowski 常数, 令 Δ 是 f 的判别式, 那么由引理 10.2 可知

$$M\leqslant\sqrt{|\Delta_K|}\leqslant\sqrt{|\Delta_K|}[O_K:\mathbb{Z}[\theta]]=\sqrt{|\Delta|}<d^dn^{1-3/2d},$$

又因为 $d\geqslant 2$, 且 $n>d^{2d^2}$, 可直接推得

$$d-1+d\log d<\frac{3}{2d}\log n\ ,\quad 2d\cdot(2\log n)^{d-1}<n^{3/2d}.$$

所以

$$\begin{aligned}[V:{K^*}^2]&\leqslant[O_K:\mathbb{Z}[\theta]]\cdot\frac{d!}{d^d}\left(\frac{4}{\pi}\right)^{r_2}\cdot\sqrt{|\Delta_K|}\frac{\left(d-1+\log\sqrt{|\Delta|}\right)^{d-1}}{(d-1)!}2^{d-r_2}\\ &=\frac{\sqrt{|\Delta|}}{d^{d-1}}2^d\left(d-1+d\log\sqrt{|\Delta|}\right)^{d-1}\cdot\left(\frac{2}{\pi}\right)^{r_2}\\ &<n^{1-3/2d}\cdot d\cdot 2^d\left(d-1+d\log d+\left(1-\frac{3}{2d}\right)\log n\right)^{d-1}\\ &<n^{1-3/2d}\cdot 2d(2\log n)^{d-1}<n,\end{aligned}$$

证毕.

3. 特殊数域筛法

特殊数域筛法的特殊性是假设 $O_K = \mathbb{Z}[\theta]$ 是唯一分解整环, 由习题 6.13 知, 这等价于 O_K 是主理想整环. 此时, 对代数筛法有更精确的描述. 首先求出所有一次素理想 (p, r) $(p \leqslant y)$ 的生成元 π, 这些 π 的全体构成集合 G. 由上述筛法就可知: 对 $(a,b) \in T_2$, 能求出 $\mu_\pi \in N$ 使得 $a+b\theta$ 和 $\prod\limits_{\pi\in G} \pi^{\mu_\pi}$ 相伴, 即相差 U_K 中的一个元素. 由 6.2 节可知, 存在算法可计算出一个基本单位系 $\varepsilon_1, \cdots, \varepsilon_r (r = r_1 + r_2 - 1)$ 和 W_K 的一个生成元 ε_{r+1}, 那么

$$a + b\theta = \prod_{i=1}^{r+1} \varepsilon_i^{\lambda_i} \cdot \prod_{\pi\in G} \pi^{\mu_\pi} \tag{10.5}$$

用对数嵌入映射 λ 作用上式, 得

$$\lambda(a+b\theta) - \sum_{\pi\in G} \mu_\pi \lambda(\pi) = \sum_{i=1}^{r} \lambda_i \lambda(\varepsilon_i).$$

因为 $\{\lambda(\varepsilon_i)\}_{1\leqslant i\leqslant l}$ 是线性无关向量, 故求解上述线性方程组, 即可给出具体的 λ_i. 对 λ_{r+1} 的确定只需比较式 (10.5) 左右两边复数的辐角即可. 特别地, θ 是实数时, $\varepsilon_{r+1} = -1, \lambda_{r+1}$ 的取值只需看式 (10.5) 左右已知实数的正负号即可. 这样, 便有如下的特殊数域筛法, 令

$$\begin{aligned} T &= T_1 \cap T_2 \\ &= \big\{(a,b)\big|\, \gcd(a,b) = 1,\, |a| \leqslant u,\, 0 < b < u,\, (a+bm)N(a+bm)\text{是 } y\text{-光滑的}\big\}, \end{aligned}$$

定义

$$\begin{aligned} &B = \pi(y); \\ &B' = \big|\{(p,r) = (\pi)\big| p \leqslant y, \text{是素数}, r \in R(p)\}\big|; \\ &B'' = r_1 + r_2; \\ &G = \{p_1, \cdots, p_B\}\text{是有理筛法的因子基, 即 } p_i \text{ 素数, 且 } p_1 < \cdots < p_B \leqslant y; \\ &\Pi = \big\{\pi_1, \cdots, \pi_{B'}\big|\pi_i\text{是范数不大于}y\text{的一次素理想的生成元}\big\}; \\ &\Sigma = \big\{\varepsilon_1, \cdots, \varepsilon_{B''}\big|\varepsilon_1, \cdots, \varepsilon_{B''-1}\text{是一基本单位系}, \varepsilon_{B''}\text{是 } W_K \text{ 的生成元}\big\}; \end{aligned}$$

Π 和 Σ 构成了代数筛法的因子基, 为明确起见, 将式 (10.5) 写成

$$a + b\theta = \prod_{i=1}^{B''} \varepsilon_i^{\lambda_i(a+b\theta)} \prod_{j=1}^{B'} \pi_j^{\mu_j(a+b\theta)}.$$

构造映射

$$
\begin{aligned}
e: T &\longrightarrow F_2^{1+B+B'+B''}\\
(a,b) &\longmapsto (e_i)_{1\leqslant i\leqslant B+B'+B''},
\end{aligned}
$$

其中

$$
e_0=\begin{cases}0, & a+bm>0,\\ 1, & a+bm<0;\end{cases}
$$

$$
\begin{aligned}
&e_i=v_{p_i}(a+bm)\,(\bmod\ 2),\quad 1\leqslant i\leqslant B;\\
&e_{B+i}=\mu_i(a+b\theta)\,(\bmod\ 2),\quad 1\leqslant i\leqslant B';\\
&e_{B+B'+i}=\lambda_i(a+b\theta)\,(\bmod\ 2),\quad 1\leqslant i\leqslant B''.
\end{aligned}
$$

若选取 T 使得 $|T|>1+B+B'+B''$, 那么用求 F_2 上线性方程组解的算法可获得一个非零集合 $S\subseteq T$ 使得

$$
\sum_{(a,b)\in S} e(a,b)=0.
$$

这样,

$$
\prod_{(a,b)\in S}(a+bm)\text{ 是 }\mathbb{Z}\text{ 中的平方元},
$$

$$
\prod_{(a,b)\in S}(a+b\theta)\text{ 是 }O_K\text{ 中的平方元}.
$$

4. **二次特征** (Adelman **方法**)

首先考虑一个比较简单的问题, 以给我们启迪. $\mathbb{Z}$ 中一个非零整数 a 是 $\mathbb{Z}$ 中的平方元, 当且仅当 $a>0$, 且对任意素数 $p\,(p\nmid a)$, $\left(\dfrac{a}{p}\right)=1$. 设 X 是 $\mathbb{Z}$ 中的一些素数构成的有限集, 若对任意不在 X 中的素数 p, 均有 Legendre 符号 $\left(\dfrac{a}{p}\right)=1$, 试问此时 a 是否是平方元, 或它离平方元有多远呢? 对 $\mathbb{Q}$ 中的元素 a 是平方元当且仅当 $a>0$, 且 $\nu_p(a)\equiv 0(\bmod\ 2)$ 对所有素数 p. 记

$$
V_X=\left\{a\in\mathbb{Q}|\ \nu_p(a)\equiv 0\,(\bmod\ 2)\text{对任意}p\notin X\right\},
$$

那么 $V_X/\mathbb{Q}^{*^2}$ 看成 F_2-线性空间维数为 $|X|+1$, 且有代表元集 $\{(-1)^{e_0}p_1^{e_1}\cdots p_g^{e_g}\,|\,e_i\in\{0,1\}, X=\{p_1,\cdots,p_g\}\}$, 对任意素数 $p\notin X$, Legendre 符号$\left(\dfrac{\cdot}{p}\right)$ 自然可看成是 $V_X/\mathbb{Q}^{*^2}$ 上的线性映射, 称作 Legendre 特征. 而 $V_X/\mathbb{Q}^{*^2}$ 的对偶空间 (即全体线性映射构成的集合) 有维数为 $|X|+1$. 如果将$\left(\dfrac{\cdot}{p}\right)$ $(p\notin X)$ 看成 V_X/Q^{*^2} 上的随机的

线性映射, 那么只要取适当多的 Legendre 特征, 就可能构成 V_X/Q^{*^2} 的对偶空间的一组基. 假若在这组基下, 对 a 的作用均为 1, 那么 a 就一定是平方元.

引理 10.7 令 k,r 是非负整数, E 是 F_2 上 k 维向量空间, 那么, 用以一致分布随机独立地从 E 中取 $k+r$ 个元素, 使其构成 E 的一个生成元集 (即包含一组基) 的概率至少是 $1-2^{-r}$.

证明 $k+r$ 个元素不构成 E 的一个生成元集当且仅当它们属于某个超平面, 而每个超平面都唯一由某个非零的线性映射 $\varphi: E\to F_2$ 所确定, 确切地说是该线性映射的核 $\ker\varphi$. 故超平面有 2^k-1 个, 对固定的一个超平面 H, 它将 E 分成两个具有相同元素个数的块, 因此 $k+r$ 个元素完全落在 H 上的概率为 $2^{-(k+r)}$, 故 $k+r$ 个元素不构成 E 的一个生成元集的概率为

$$(2^k-1)\cdot 2^{-k-r} < 2^{-r},$$

等价地说, $k+r$ 个元素构成 E 的概率至少是 $1-2^{-r}$, 证毕.

由引理 10.7 知, 只要有一种选取 Legendre 特征的方法, 使一个元素 $a\in\mathbb{Z}$ 能够通过足够多的 Legendre 特征的判别, 就能确信它是一个平方元. 现在用 $\mathbb{Z}[\theta]$ 来替换 $\mathbb{Z}$, 创建类似的方法来判别一些 $a+b\theta$ 的乘积是否是平方元.

引理 10.8 令 S 是一些互素的整数对 (a,b) 构成的有限集, 且 $\prod\limits_{(a,b)\in S}(a+b\theta)$ 是 K 中的平方元, q 是奇素数, $s\in R(q)$, 使得

(1) 对任意 $(a,b)\in S, a+bs\not\equiv 0(\mathrm{mod}\ q)$;

(2) $f'(s)\not\equiv 0(\mathrm{mod}\ q)$,

那么 $\prod\limits_{(a,b)\in S}\left(\dfrac{a+bs}{q}\right)=1$.

证明 令

$$\begin{aligned}\varphi:\mathbb{Z}[\theta]&\longrightarrow F_q\\ \theta&\longmapsto s\end{aligned}$$

是环同态. 显然 $\mathfrak{P}=\ker\varphi$ 是一次素理想, 由 q 和 s 完全确定, 定义映射

$$\begin{aligned}\chi_{\mathfrak{P}}:\mathbb{Z}[\theta]-\mathfrak{P}&\longrightarrow F_q^* &&\longrightarrow \{\pm1\}\\ g(\theta)&\longmapsto g(s)&&\longmapsto \left(\frac{g(s)}{q}\right),\end{aligned}$$

显然 $\chi_{\mathfrak{P}}$ 保持乘法运算. 由引理 6.3 可知, 存在 $\delta\in\mathbb{Z}[\theta]$ 使得 $f'(\theta)^2\prod\limits_{(a,b)\in S}(a+b\theta)=\delta^2$. 由条件知 $\delta\notin\mathfrak{P}$, 故在上式两边作用 $\chi_{\mathfrak{P}}$, 可得

$$\prod_{(a,b)\in S}\left(\frac{a+bs}{q}\right)=1,$$

证毕.

最感兴趣的是引理 10.8 的逆命题, 假若一个元素 $\beta \in \mathbb{Z}[\theta] - \{0\}$, 满足除有限个一次素理想外, 对所有满足 $2\beta \notin \mathfrak{P}$ 的一次素理想 $\mathfrak{P}$, 均有 $\chi_{\mathfrak{P}}(\beta) = 1$, 那么 β 是 K 中的平方元的可能性有多大?

由于文献 [6] 告诉我们, 一定有一个由 $\mathbb{Z}[\theta]$ 的素理想构成的有限集 X, 使得对任一不在 X 中的一次素理想 $\mathfrak{P}$, 上述的映射 $\chi_{\mathfrak{P}}$ 均能诱导出 $V/{K^*}^2 \to \{\pm 1\}$ 的一个同态映射.

下面在 $O_K = \mathbb{Z}[\theta]$ 时, 具体解释这一结论, 此时 $V = W$.

令 $Cl(O_K)^{[2]}$ 是类群 $Cl(O_K)$ 中所有二阶元全体, 显然 $Cl(O_K)^{[2]}$ 可看成 F_2-向量空间, 设其维数为 e, 且 $\overline{\mathfrak{a}}_1, \cdots, \overline{\mathfrak{a}}_e$ 是其一组基, $\mathfrak{a}_i$ 是 O_K 的理想, 那么存在 $r_i \in O_K$ 使得 $\mathfrak{a}_i^2 = r_i O_K$, 令

$$\Omega = \{2, r_1, \cdots, r_e, f'(\theta)\}.$$

设 X 是包含 Ω 中某个元素的所有一次素理想构成的有限集, 再设 $\varepsilon_0, \varepsilon_1, \cdots, \varepsilon_{r_1+r_2-1}$ 是 O_K^* 的生成元集, 和定理 10.2 的证明过程一样, 可以证明存在群的正合列

$$1 \longrightarrow O_K^*/{O_K^*}^2 \longrightarrow W/{K^*}^2 \longrightarrow Cl(O_K)^{[2]} \longrightarrow 1.$$

由此可知

$$\{\varepsilon_0^{a_0}\varepsilon_1^{a_1}\cdots\varepsilon_{r_1+r_2-1}^{a_{r_1+r_2-1}} r_1^{b_1}\cdots r_e^{b_e} \mid a_i, b_j \in \{0,1\}\}$$

是有限群 $W/{K^*}^2$ 的一个代表元集. 故对任意不属于 X 的一次素理想 $\mathfrak{P}$, 将 $\chi_{\mathfrak{P}}$ 自然看成从 $W/{K^*}^2$ 到 $\{\pm 1\}$ 的同态映射, $\chi_{\mathfrak{P}}$ 便是 $V/{K^*}^2$ 的对偶空间中的元素. 由 Cebotarer 密度定理 (参见文献 [26]) 可知, 若 $\mathfrak{P}$ 跑遍 $\mathbb{Z}[\theta]$ 的所有不在 X 中的一次素理想, $\chi_{\mathfrak{P}}$ 渐近在 $\hom(V/{K^*}^2, \{\pm 1\})$ 均匀分布, 而由定理 10.2 知

$$\dim_{F_2}(\hom(V/{K^*}^2, \{\pm 1\})) \leqslant \log n/\log 2.$$

概括引理 10.7 只要 $\mathfrak{P}$ 取充分多 (至少大于 $\log n/\log 2$), 就可以有很大的概率得证 $\{\chi_{\mathfrak{P}}\} = U$ 构成 $\hom(V/{K^*}^2, \{\pm 1\})$ 的一组基. 若 $\beta \in \mathbb{Z}[\theta]$ 对所有 $\chi_{\mathfrak{P}} \in U$, $\chi_{\mathfrak{P}}(\beta) = 1$, 那么, 就可以有很大的概率得证 β 是 O_K 中的平方元. Adelman 建议 $|U| \sim 3 \cdot \log n/\log 2$, 这样, 便有如下的算法策略: 令

$$\begin{aligned} T = T_1 \cap T_2 = &\{(a,b) \mid \gcd(a,b) = 1, |a| \leqslant u, \\ &0 < b \leqslant u, (a+bm)N(a+b\theta) \text{是 } y\text{-光滑的}\}, \end{aligned}$$

定义

$$
\begin{aligned}
&B=\pi(y);\\
&B'=|\{(p,r)|\ p\leqslant y,\text{是素数},r\in R(p)\}|;\\
&B''=[3\log n/\log 2];\\
&\{p_1,\cdots,p_B\}\text{是有理筛法的因子基, 即}p_i\text{素数, 且}p_1<\cdots<p_B\leqslant y;\\
&\{(p_1,r_1),\cdots,(p_{B'},r_{B'})\}\text{是代数筛法的因子基};\\
&\{(q_1,s_1),\cdots,(q_{B''},s_{B''})\}\text{是 } B'' \text{ 个 } \mathbb{Z}[\theta] \text{ 中一次素理想构成的集合},\\
&\qquad y<q_1\leqslant\cdots\leqslant q_{B''},\quad \text{且} f'(s_i)\neq 0\,(\mathrm{mod}\ q)_i,\quad 1\leqslant i\leqslant B'';
\end{aligned}
$$

构造映射

$$
\begin{aligned}
e:T&\longrightarrow F_2^{1+B+B'+B''}\\
(a,b)&\longmapsto(\cdots,e_i,\cdots)_{0\leqslant i\leqslant B+B'+B''},
\end{aligned}
$$

其中

$$
\begin{aligned}
&e_0=\begin{cases}0, & a+bm>0,\\ 1, & a+bm<0;\end{cases}\\
&e_i=\nu_{p_i}(a+bm)\,(\mathrm{mod}\ 2),\quad 1\leqslant i\leqslant B;\\
&e_{B+i}=e_{p_i,r_i}(a+b\theta),\quad 1\leqslant i\leqslant B';\\
&e_{B+B'+i}=\begin{cases}0, & \left(\dfrac{a+bs_i}{q_i}\right)=1,\\ 1, & \left(\dfrac{a+bs_i}{q_i}\right)=-1,\end{cases}\quad 1\leqslant i\leqslant B''.
\end{aligned}
$$

若选取 T 使得 $|T|>1+B+B'+B''$, 那么用 F_2 上求线性方程组解的算法可以获得一个非空子集合 $S\subseteq T$ 使得

$$\sum_{(a,b)\in S}e(a\ b)=0.$$

这样,

$$\prod_{(a,b)\in S}(a+bm)\text{是 } \mathbb{Z} \text{ 中的平方元},$$

$$\prod_{(a,b)\in S}(a+b\theta)\text{几乎是 } O_K \text{ 中的平方元},$$

即

$$f'(\theta)\prod_{(a,b)\in S}(a+b\theta)\text{几乎是 } \mathbb{Z}[\theta] \text{ 中的平方元}.$$

5. 求平方根

由于知道 $a+bm$ 的素数分解, 所以

$$f'(m)^2 \prod_{(a,b)\in S}(a+bm)$$

在 $\mathbb{Z}$ 中的平方根是容易获得的. 而

$$r = f'(\theta)^2 \prod_{(a,b)\in S}(a+b\theta)$$

是 $\mathbb{Z}[\theta]$ 中的平方元, 要求 r 的平方根, 首先将乘积展开, 且利用 $f(\theta)=0$, 将 r 写成关于 θ 的次数 $< d$ 的整系数多项式 $B(\theta)$, 然后, 可利用代数数域上多项式的分解算法, 去获得 $x^2-r\in K(x)$ 的解. 然而, 由于 S 的尺寸和 $B(\theta)$ 的系数非常大, 计算 $B(\theta)$ 就要花费很多时间及很大的存储空间, 分解 x^2-r 的时间就更多, 为此, 要寻找其他方法.

假若 q 是个奇素数, 且 $f(x)(\mathrm{mod}\ q)$ 是 F_q 上不可约多项式 (用附录中算法 1.1 判别), 那么

$$\mathbb{Z}[\theta]/q\mathbb{Z}[\theta] \cong F_q[x]/(f(x) \bmod q) = F_{q^d}.$$

令 $\mathfrak{P}=q\mathbb{Z}[\theta]$ 是 $\mathbb{Z}[\theta]$ 中的 d 次素理想, 因为 $f(x)(\mathrm{mod}\ q)$ 不可约的, 所以 $f'(\theta)\notin\mathfrak{P}$, 又因 $(a,b)=1$, 自然 $(a+b\theta)\notin\mathfrak{P}$, 故 $r\notin\mathfrak{P}$.

$r(\mathrm{mod}\ q)$ 事实上就是将 r 的系数模 q, 看成 F_{q^d} 中的元素, 利用有限域上求平方根算法, 就能获得 $\delta_0(\mathrm{mod}\ q)$, 使得

$$\delta_0^2 r \equiv 1\,(\mathrm{mod}\ q),$$

事实上, δ_0 是 r 的一个平方根的逆, 忽略正负号是唯一确定的, 利用牛顿迭代公式, 对 $j\geqslant 1$ 计算

$$\delta_j = \frac{\delta_{j-1}(3-\delta_{j-1}^2 r)}{2}\,(\mathrm{mod}\ q)^{2^j},$$

容易验证 δ_j 满足 $\delta_j^2 r\equiv 1(\mathrm{mod}\ q)^{2^j}$, 一旦 j 充分大, 是 $q^{2^j}>r$ 的确切平方根 β 的重数绝对值最大值的 2 倍, 计算 $\beta=\delta_j r(\mathrm{mod}\ q)^{2^r}$ 便得到 r 在 $\mathbb{Z}[\theta]$ 中的平方根.

当 d 是奇数时, Couveignes 用多个模数和中国剩余定理给出了一个更好的算法[12].

值得注意的是, 对特定 $f(x)$, 不一定存在素数 q, 使 $f(x)(\mathrm{mod}\ q)$ 是 $F_q[x]$ 中不可约多项式 (如 $f(x)=x^4+1$), 此时一般的方法是寻找新的 $f(x)$, 然后取 $q=2, 3, 5, \cdots$ 去判别 $f(x)(\mathrm{mod}\ q)$ 是否不可约, 如果这样的 q 存在, 有多少呢?

引理 10.9　令 $f(x) \in \mathbb{Z}[x]$ 是 $d > 1$ 次不可约多项式, 那么在所有素数中, 满足 $f(x) (\bmod\ q) \in F_q[x]$ 没有线性因子的素数 q 所占的比例 $\geqslant \frac{1}{d}$.

证明　由于 d 一般是较小的, 所以这样的 q 是容易找的.

6. 复杂度分析

整个数域筛法的时间复杂度分析涉及每个子块的时间复杂度, 主要是多项式的选取、筛法、线性方程组的求解、代数平方根的求解以及一些参数的选取. 筛法是数域筛法中最耗时的部分, 其耗时的多少在很大程度上依赖于 $f(x)$ 的选取; 通过筛法过滤后得到的大规模稀疏方程组 (即方程中出现的变元个数很少), 常用 Lanczos 算法[27,36] 去求解. 最后求代数的平方根, 还常用有 Pguyen 的方法[39]. 具体的时间复杂度分析要用一些解析数论的结果, 本书省略这点, 感兴趣的读者参阅文献[6].

习　题

习题 10.1　用连分式算法分解 9509 和 13561.

习题 10.2　令 $n = 199843247$, 利用椭圆曲线 $E: y^2 = x^3 + 53x - 53$, 点 $P = (1, 1)$ 和整数 $k = 16296$, 用 Lenstra 算法通过计算 kP 去分解 n.

第 11 章　椭圆曲线上的离散对数

11.1　椭圆曲线公钥密码

以下通过椭圆曲线公钥密码来说明这个概念及其应用.

设 E 为定义在有限域 F_q 上的椭圆曲线, 为简单起见, 以下假定 $q \neq 2,3$ 为一素数. 在 $E(F_q)$ 中选一个点 P, 称为基点, 记 P 的阶为 n, 通常要求 n 是一个大素数 (其理由见 11.2 节). 每个用户选取一个整数 e $(1 \leqslant e < n)$ 作为其私钥, 而以点 $D = eP$ 作为其公钥, 这样就形成一个椭圆曲线公钥密码系统 (ECC). 定义 E 的方程 $y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0)$, 基域 F_q, 基点 P 及其阶 n, 以及每个用户的公钥都是该系统的公开参数. 每个用户的私钥都是保密的, 仅本人知道.

假设用户 A 欲将明文 m $(0 < m < q)$ 加密后发送给 B, A 首先要查得 B 的公钥 D_B, 然后进行以下的加密运算:

(1) 取随机数 $k \in \mathbb{Z}$ 计算 $kP = (x_1, y_1)$(今后将 $[k]P$ 简写为 kP);

(2) 计算 $kD_B = (x_2, y_2)$;

(3) 计算密文 $c = m \oplus x_2$(将 m 和 x_2 用二进制表示, 然后按位模 2 加), 将 (c, x_1, y_1) 发送给 B.

B 收到 A 发来的信息后, 进行下述的运算:

(1) 计算 $e_B(x_1, y_1) = (x_2, y_2)$, e_B 为 B 的私钥;

(2) 计算 $m = c \oplus x_2$, 得到明文 m.

因为 $e_B(x_1, y_1) = e_B kP = kD_B = (x_2, y_2)$, 上述解密是正确的.

公钥密码另一个重要用途是进行数字签名. 在计算机网络通信中, 数字签名可用于确认发信人的身份; 发现在传输过程中, 信息 m 是否被非法窜改; 具有不可抵赖不可更改性. 以下介绍基于椭圆曲线的数字签名方案 (ECDSA).

假设用户 A 对信息 m(为简单起见, 这里不妨假设 $0 < m < q$) 作数字签名, A 随机选取 $k \in \mathbb{Z}$, 计算 kP, 令 $r = x(kP)$ (kP 的 x 坐标), 计算 s, 它适合

$$sk \equiv m + re_A \pmod{n}$$

(e_A 是 A 的私钥), 则 (m, r, s) 就是签名后 A 发出的报文.

任一用户收到 A 发出的 (m, r, s), 查得 A 的公钥 D_A, 计算 $s^{-1} \pmod{n}$, 检验

$$r = x(s^{-1}(mP + rD_A))$$

是否成立, 如果成立, 签名得到验证; 否则, 不能通过验证. 由于 $skP = mP+re_AP = mP + rD_A$, 所以 $kP = s^{-1}(mP + rD_A)$, 上述验证显然是正确的. 只有 A 才知道他的私钥 e_A, 任何第三者要假冒 A 的签名, 或更改经 A 签名后的信息, 都是难于通过验证的. A 对信息签名后, 也是不能否认的.

已知 E 的点 D 是 P 的倍数, 求整数 $l \in \mathbb{Z}$ 使得 $D = lP$, 这称为椭圆曲线的离散对数问题 (ECDLP). ECC 的安全性是建立在椭圆曲线离散对数计算难度基础之上, 如果离散对数可以计算, 从一个用户的公钥就可得到他的私钥, ECC 就不安全了. 本章以下内容集中研究椭圆曲线离散对数的计算问题.

在应用椭圆曲线公钥密码时, 最主要的计算量用于计算 kP. 今以 $F_p(p > 3$ 为素数) 上的椭圆曲线为例, 说明如何计算 kP. 在 7.1 节的开头, 我们已讲过, 椭圆曲线上的点可以用射影坐标 (X, Y, Z) 或仿射坐标 $x = X/Z, y = Y/Z$ 表示, 现在再引进一个新的坐标 (称为 Jacobi 坐标), 令 $x = X/Z^2, y = Y/Z^3$, 它适合方程

$$Y^2 = X^3 + aXZ^4 + bZ^6,$$

该方程与方程 (7.4) 的齐次形式

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

显然定义同一条曲线. 以下将会看到, 使用不同的坐标, 计算椭圆曲线上两点之和 $P + Q$ 与倍点 $2P$ 的计算量是不同的. 以 S, M, I 分别表示 F_p 中进行一次平方运算、乘法运算和求逆运算所需的时间 (几乎对所有的域 F_p, S 约为 $0.8M$, 而 I/M 随着基域 F_p 的不同, 以及算法实现的不同而有所变化, 当 $|p| > 100$ 比特时, 估计 I/M 在 9.5 与 30 之间).

在 7.1 节中已经给出了仿射坐标下加法的计算公式.令 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ 及 $P + Q = (x_3, y_3)$, 当 $P \neq Q$ 时, 加法公式为

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1,$$

其中 $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

当 $P = Q$ 时, 倍点公式为

$$x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1,$$

其中 $\lambda = (3x_1^2 + a)/(2y_1)$. 易见在仿射坐标下加法运算和倍点运算所需计算量分别为 $I + 2M + S$ 和 $I + 2M + 2S$.

考虑使用射影坐标时所需计算量, 令 $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$ 及 $P + Q = (X_3, Y_3, Z_3)$, 当 $P \neq \pm Q$ 时, 容易推得其加法公式为

$$X_3 = vA, \quad Y_3 = u(v^2X_1Z_2 - A) - v^3Y_1Z_2, \quad Z_3 = v^3Z_1Z_2,$$

其中 $u=Y_2Z_1-Y_1Z_2,\ v=X_2Z_1-X_1Z_2,\ A=u^2Z_1Z_2-v^3-2v^2X_1Z_2$.

倍点公式为

$$X_3=2hs,\quad Y_3=w(4B-h)-8Y_1^2s^2,\quad Z_3=8s^3,$$

其中 $w=aZ_1^2+3X_1^2,\ s=Y_1Z_1,\ B=X_1Y_1s, h=w^2-8B$.

可见, 在射影坐标之下, 加法运算和倍点运算所需计算量分别为 $12M+2S$ 和 $7M+5S$.

最后, 考虑在 Jacobi 坐标下点的加法和倍点运算所需计算量, 令 $P=(X_1, Y_1, Z_1)$, $Q=(X_2, Y_2, Z_2)$ 及 $P+Q=(X_3, Y_3, Z_3)$, 当 $P\neq\pm Q$ 时, 容易推得其加法公式为

$$X_3=-H^3-2U_1H^2+r^2,\quad Y_3=-S_1H^3+r(U_1H^2-X_3),\quad Z_3=Z_1Z_2H,$$

其中 $U_1=X_1Z_2^2,\ U_2=X_2Z_1^2,\ S_1=Y_1Z_2^3,\ S_2=Y_2Z_1^3,\ H=U_2-U_1,\ r=S_2-S_1$.

倍点公式为

$$X_3=T,\quad Y_3=-8Y_1^4+M(S-T),\quad Z_3=2Y_1Z_1,$$

其中 $S=4X_1Y_1^2,\ M=3X_1^2+aZ_1^4,\ T=-2S+M^2$.

在 Jacobi 坐标之下, 加法运算和倍点运算所需计算量分别为 $12M+4S$ 和 $4M+6S$. 可见, 利用 Jacobi 坐标进行倍点运算速度较快. 还可以有其他一些坐标, 也可以考虑把几种坐标混合使用, 以求达到最好的效果 (参阅文献 [10]).

现在考虑如何计算 kP. 最一般的算法, 是取 k 的二进制表示 $k=\sum\limits_{j=0}^{l-1}k_j2^j,\ k_j\in\{0,1\}$, 依次做倍点计算 $2P, 4P, \cdots, 2^{l-1}P$, 然后将对应 $k_j=1$ 的那些项相加. 设 k_j $(0\leqslant j\leqslant l-1)$ 中有 w 个 1, 则该方法需做 $l-1$ 次倍点运算, $w-1$ 次加法运算. w 的平均值为 $l/2$.

设 $P=(x,y)$, 则 $-P=(x,-y)$, 这是一个可以利用的简单运算, 将 k 表为

$$\sum_{j=0}^{l-1}s_j2^j,\quad s_j\in\{-1,0,1\},$$

称为 (二进制) 带符号表示, s_j $(0\leqslant j\leqslant l-1)$ 总共有 3^{l+1} 个可能组合, 所表示的 k 可从 $-(2^{l+1}-1)$ 增至 $2^{l+1}-1$, 可见, 一个固定的 k 可以有不同的带符号表示. 例如, $3=1+2=-1+4$. 为了减少 kP 的计算量, 希望选取非零 s_j 个数最少的表示. 当一个带符号表示中任意两个相邻的 s_j 和 s_{j+1} 中至少有一个为零时, 即对任一 $0\leqslant j\leqslant l-1$ 都有 $s_js_{j+1}=0$ 时, 称该表示为无关联形式 (NAF). 可以证明任一

整数都有唯一的 NAF, 且其长度最多比它的最短带符号表示大1[37]. NAF 中非零系数的平均值为 $l/3$. 可见利用 NAF 可以减少 kP 的计算量.

关于计算 kP 的其他一些方法, 可参阅文献 [4] 的第四章.

11.2 小步-大步法

设 P 为椭圆曲线 E 上的点, P 的阶为 n, 已知点 $D \in \langle P\rangle$(P 生成的循环群), 求正整数 l, 使 $D = lP$ $(0 \leqslant l < n)$.

将 l 表为

$$l = c[\sqrt{n}\,] + d, \quad 0 \leqslant c, d < [\sqrt{n}\,],$$

这里 $[\sqrt{n}\,]$ 表示不小于 $\sqrt{n}$ 的最小正整数. 令 $R_d = D - dP$, 存储关于 R_d $(1 \leqslant d < [\sqrt{n}\,])$ 的表, 对于 $c = 0, 1, \cdots, [\sqrt{n}\,] - 1$, 依次计算 $S_c = c[\sqrt{n}\,]P$. 将 S_c 与 R_d 表中的点比较, 若某个 S_{c_0} 与 R_{d_0} 相同, 则有 $l = c_0[\sqrt{n}\,] + d_0$.

计算 R_d 可称为小步, 计算 S_c 可称为大步, 文献上将这个方法称为 "小步-大步" 方法. 它要求存储 R_d 表, 存贮量为 $O(\sqrt{n})$ 个 E 的点. 小步和大步都要求 $O(\sqrt{n})$ 次 E 上点的运算, 所以该方法的计算复杂度为 $O(\sqrt{n})$. 这是迄今为止所知道的计算任意椭圆曲线的 ECDLP 最好的复杂度.

11.3 节将介绍 Pollard 的方法[43], 它们也可用于计算任意椭圆曲线的 ECDLP, 计算复杂度也是$O(\sqrt{n})$, 但仅需要很小的存储量. 这里先介绍 Pohlig 和 Hellman[40] 处理 ECDLP 的一个方法, 它指出仅需考虑 P 的阶 n 为素数时的 ECDLP.

设 $n = \prod p_i^{c_i}$ 为标准因子分解, p_i 为素数. 若对每个 $p_i^{c_i}$ 能计算 $l(\bmod\ p_i^{c_i})$, 则由中国剩余定理就可得到 l. 令 $n_i = n/p_i^{c_i}$, 则

$$D_i = n_i D = l(n_i P) = lP_i,$$

P_i 的阶为 $p_i^{c_i}$, 因而对每个 i, 计算 n 为 $p_i^{c_i}$ 的 ECDLP 就可得到 $l(\bmod\ p_i^{c_i})$.

进一步, 设 $n = p^c$ 为素数幂, 令

$$D_0 = p^{c-1}D = l(p^{c-1}P) = lP_0,$$

P_0 的阶为 p, 计算该 $n = p$ 的 ECDLP 可得到 $l \equiv l_0(\bmod\ p)$ $(0 \leqslant l_0 < p)$. 设 $l = l_0 + l_1 p$, 则

$$D_1' = D - l_0 P = l_1(pP) = l_1 P_1',$$

P_1 的阶为 p^{c-1}. 类似地, 令

$$D_1 = p^{c-2}D_1' = l_1(p^{c-2}P_1') = l_1 P_1,$$

P_1 的阶为 p, 计算该 ECDLP 可得到 $l_1(\bmod\ p)$, 从而得到 $l(\bmod\ p^2)$. 重复使用上述方法, 可依次得到 $l(\bmod\ p^i)$ $(i = 1, 2, \cdots, c)$.

由于存在 Pohlig 和 Hellman 的方法, 在使用椭圆曲线公钥密码时, 要求选取基点 P 的阶 n 是一个大素数, 使得 $O(\sqrt{n})$ 的计算量不能实现. 因而在选取椭圆曲线时, 要求它的阶 (其上点的个数) 是一个大素数或是一个近似素数 (一个大素数与几个小素因子之积), 如何构造这样的椭圆曲线, 是一个深刻的数学问题. 由于篇幅的限制, 本书不能讲解这个问题.

本节所讨论的方法适用于任意交换群上的离散对数的计算.

11.3　家袋鼠和野袋鼠

袋鼠的跳跃看似一随机的游动, 实际上并非如此, 它每次跳跃的方向和距离都由起跳点的状态所决定. 设想在一块地里, 一只家袋鼠带一把铲子, 它每跳十步就在所到达的地方挖一个洞, 并把洞口伪装起来. 之后如果一只野袋鼠进入同一块地里, 只要它一旦碰到家袋鼠的足迹, 则它最多跳十步就会掉入一个洞中. 这个家袋鼠逮野袋鼠的方法, 可用于计算离散对数.

设 G 为 n 阶有限交换群, $P, D \in G$ 且 $D = mP$, 要计算 m. 定义函数

$$f : G \longrightarrow \{1, 2, \cdots, s\},$$

s 是一个可以选择的正整数. 假设 f 是一致分布的, 即

$$\sum_{i=1}^{s} \left| \#\{g \in G | f(g) = i\} - \frac{n}{s} \right| = O(\sqrt{n}).$$

令

$$M_i = a_i P + b_i D, \quad a_i, b_i \in \mathbb{Z}, \quad i = 1, 2, \cdots, s,$$

定义函数

$$\begin{aligned} F : G &\longrightarrow G \\ g &\longmapsto g + M_{f(g)}, \end{aligned}$$

从 g_0 出发, 通过 $g_k = F(g_{k-1})$ 就可得到一个随机游动.

上述家袋鼠逮野袋鼠的方法为: 在 G 中取两点

$$g_0 = x_0 P + x_0' D, \quad h_0 = y_0 P + y_0' D.$$

利用以上通过 F 定义的游动计算

$$g_k = x_k P + x_k' D, \quad h_k = y_k P + y_k' D, \quad k = 1, 2, \cdots.$$

如果能找到 i, l 使 $g_i = h_l$, 则有 $x_i P + x_i' D = y_l P + y_l' D$, 从而 $(x_i' - y_l')D = (y_l - x_i)P$, 当 $x_i' - y_l'$ 与 n 互素时, 即可得到 m. 实际上, 在计算过程中若出现某两个 g_k 相同, 或某两个 h_k 相同, 也有可能得到离散对数 m.

粗略地估计一下该方法所需要的计算量, 计算 g_0, h_0 后, $g_0 \neq h_0$ 的概率为 $1-\frac{1}{n}$, 计算 g_1 后, $g_1 \neq g_0, h_0$ 的概率为 $1-\frac{2}{n}$, 计算 h_1 后, $h_1 \neq g_0, g_1, h_0$ 的概率为 $1-\frac{3}{n}$, 依此类推, 在计算 $g_0, \cdots, g_{k-1}, h_0, \cdots, h_{k-1}$ 后, 其中不出现两个相同的元素的概率为

$$\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{2k}{n}\right) \sim 1-\frac{1}{n}\sum_{i=1}^{2k} i$$

(当 n 很大时), 因而出现两个相同元素的概率约为 $k(2k-1)/n$, 可见所需计算量为 $O(\sqrt{n})$.

为了发现 $\{g_k\}$ 与 $\{h_k\}$ 之间的碰撞, 可将所计算的 g_k 和 h_k 都存储起来, 但这样所需的存储量较大. 为了减少存储量, 定义 G 上的一个函数

$$H: G \longrightarrow \mathbb{Z},$$

当 $H(g)$ 具有某种性质时, 例如, 它的二进制表达式中最底的 i 位都为零时, 称 g 为判别元. 仅存储 g_k 和 h_k 中的判别元, 寻找判别元之间的碰撞, 这时存储量为原来的 $1/2^i$, 但计算量将平均增加 2^i 倍, 在将该方法用于 ECDLP 时, 可以取 g 的 x 坐标作为 $H(g)$.

11.4 MOV 约化

MOV 约化是由 Menezes, Okamoto 和 Vanstone 提出来的一个计算 ECDLP 的方法[34], 设 E/F_q 为椭圆曲线, 点 $P \in E(F_q)$ 的阶为 n, 假设 n 与 q 互素 (这是应用中最常见的情况), 已知 $D \in \langle P\rangle$ 计算 l 使 $D = lP$.

假设 k 为最小正整数, 使 $E[n] \subset E(F_{q^k})$, 因而 F_{q^k} 中包含 n 次单位根 μ_n(定理 7.14).

引理 11.1 设 $P_1, P_2 \in E[n]$, 则 $e_n(P, P_1) = e_n(P, P_2)$ 的充分必要条件是 P_1 和 P_2 属于子群 $\langle P\rangle$ 在 $E[n]$ 中的同一陪集.

证明 若 P_1 与 P_2 属于 $\langle P\rangle$ 的同一陪集, 存在正整数 k 使 $P_1 = P_2 + kP$, 则

$$e_n(P, P_1) = e_n(P, P_2 + kP) = e_n(P, P_2)e_n(P, P)^k = e_n(P, P_2).$$

若 P_1 与 P_2 属于不同的陪集, 因 $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ (定理 7.12), 可找到 $Q \in E[n]$, 使 Q, P 为 $E[n]$ 的一组基, 因而 $P_1 - P_2 = a_1P + a_2Q$, 且 $a_2Q \neq \mathcal{O}$. 设 $b_1P + b_2Q$ 为 $E[n]$ 的任一点, 则

$$e_n(a_2Q, b_1P + b_2Q) = e_n(a_2Q, P)^{b_1} e_2(Q, Q)^{a_2b_2} = e_n(a_2Q, P)^{b_1},$$

可见 $e_n(a_2Q,P)\neq 1$, 否则将有 $a_2Q=\mathcal{O}$(定理 7.13 的 (3)). 从而

$$e_n(P,P_1)e_n(P,P_2)^{-1}=e_n(P,a_1P+a_2Q)=e_n(P,a_2Q)\neq 1,$$

证毕.

定理 11.1　*设 $P\in E[n]$, 一定存在 $Q\in E[n]$, 使 $e_n(P,Q)$ 为 n 次本原单位根.*

证明　$\langle P\rangle$ 在 $E[n]$ 中有 n 个不同的陪集, 对任一 $Q\in E[n]$, $e_n(P,Q)$ 为 n 次单位根, 由引理 11.1, 当 Q 跑遍 n 个不同的陪集时, $e_n(P,Q)$ 跑遍所有的 n 次单位根, 证毕.

设 $\alpha=e_n(P,Q)\in F_{q^k}$ 为 n 次本原单位根, 记 $\beta=e_n(D,Q)\in F_{q^k}$. 若在 F_{q^k} 中能计算以 α 为基 β 的离散对数 l, 即 $\beta=\alpha^l$, 则

$$e_n(D,Q)=e_n(P,Q)^l=e_n(lP,Q),$$

令 $D-lP=sP$, 从而

$$e_n(P,Q)^s=e_n(sP,Q)=e_n(D,Q)\cdot e_n(P,Q)^{-l}=1,$$

由于 $e_n(P,Q)$ 为 n 次本原单位根, 可见 $n|s, D=lP$.

上述方法将椭圆曲线上离散对数的计算归结为有限域 F_{q^k}上离散对数的计算, 这个约化过程包括以下两个步骤:

(1) 找到最小的正整数 k, 使 $E[n]\subset E(F_{q^k})$;

(2) 找到点 $Q\in E[n]$, 使 $e_n(P,Q)$ 为 n 次本原单位根. (11.1)

可以利用式 (7.18) 计算 Weil 对. 关于 $f_T(D_S)$ 的计算, 式 (7.13) 的推导过程实际上给出了计算函数 f_T 使 $\mathrm{div}(f_T)=n(T)-n(\mathcal{O})$ 的方法, 但在这里并不一定要计算函数 f_T, 而是要计算它在某些点的值. 假设要计算 $f_T(S)$, 定义 $\langle T\rangle\times F_q^*$ 上的一个群运算:

$$(r_1T,a_1)\oplus(r_2T,a_2)=\big((r_1+r_2)T,a_1a_2h(S)\big),$$

其中

$$\mathrm{div}(h)=(r_1T)+(r_2T)-\big((r_1+r_2)T\big)-\big(\mathcal{O}\big).$$

设 $n=\alpha_0+2\alpha_1+\cdots+2^s\alpha_s$ $(\alpha_i=0,1)$, 从 $(T,1)$ 出发, 依次计算

$$(2T,a_1),\quad (4T,a_2),\cdots,\quad (2^sT,a_s),$$

其中

$$a_i=f_i(S),\quad \mathrm{div}f_i\sim 2^i(T)-(2^iT)-(2^i-1)(\mathcal{O}),$$

然后计算

$$\alpha_0(T,1)\oplus\alpha_1(2T,a_1)\oplus\cdots\oplus\alpha_s(2^sT,a_s)=(\mathcal{O},f_T(S)).$$

以 $R(n)$ 表示上述计算进程中出现的 iT $(0\leqslant i<n)$ 的集合, 只要 $S\notin R(n)$, 上述计算是可行的. 若计算 $f_T(D_S)$, 只要找到整数 k, 使 $(k+1)S$ 与 kS 都不在 $R(n)$ 中出现, 取 $D_S=\big((k+1)S\big)-(kS)\sim(S)-(\mathcal{O})$, 则 $f_T(D_S)=f_T\big((k+1)S\big)/f_T(kS)$. 计算 $f_T(S)$ 的计算量为 $O(\log n)$.

下面就一类特殊的椭圆曲线 —— 超奇异椭圆曲线, 讨论如何利用 MOV 约化.

设 F_q 的特征为 p, 当 E/F_q 的 q 阶 Frobenius 变换的迹 t 是 p 的倍数时, E 称为超奇异的.

我们有 $|q+1-\#E(F_q)|\leqslant 2\sqrt{q}$(定理 7.16). 反之, 若 $|t|\leqslant 2\sqrt{q}$, 是否存在椭圆曲线 E/F_q, 使 $\#E(F_q)=q+1-t$?

定理 11.2 设 $q=p^m$, 当且仅当 t 适合下述条件之一时, 存在椭圆曲线 E/F_q, 使 $\#E(F_q)=q+1-t$:

(1) $p\nmid t$, $t^2\leqslant 4q$;

(2) m 是奇数, 下列条件之一成立:

(a) $t=0$;

(b) $t^2=2q$, $p=2$;

(c) $t^2=3q$, $p=3$;

(3) m 是偶数, 下列条件之一成立:

(a) $t^2=4q$;

(b) $t^2=q$, $p\not\equiv 1(\bmod 3)$;

(c) $t=0$, $p\not\equiv 1(\bmod 4)$.

证明 见文献 [47].

由定理 11.2 可知, 当且仅当 $t^2=0,q,2q,3q,4q$ 时, E 为超奇异椭圆曲线.

设 K 为 $\mathbb{Q}$ 上的虚二次域, $O_{\max}$ 表示 K 中的代数整数环, $1,\omega$为它在 $\mathbb{Z}$ 上的一组基. $O_{\max}$ 中任一形如 $O=\mathbb{Z}+k\omega\mathbb{Z}$($k$ 为任一正整数) 的子环, 称为阶 (order), O 的判别式 $\Delta(O)=\Delta(O_{\max})k^2$, 所以 O 也由它的判别式唯一决定, 以 $O(\Delta)$ 表示判别式为 Δ 的阶.

定理 11.3 F_q 的特征为 p, 正整数 n 与 p 互素, E/F_q 上的 q 阶 Frobenius 变换 ϕ 的迹为 t, 则下述条件等价:

(1) $E[n]\subset E(F_q)$;

(2) $n^2|\ q+1-t,\ n|q-1,\ \phi\in\mathbb{Z}$ 或 $O\left(\dfrac{t^2-4q}{n}\right)\subset \mathrm{End}_{F_q}(E)$.

$\mathrm{End}_{F_q}(E)$ 是定义在 F_q 上的 E 的同种映射组成的环.

证明 因 $\mathrm{Ker}(\phi-1)=E(F_q)$, $\mathrm{Ker}([n])=E[n]$, 条件 (1) 成立的充分必要条件为 (定理 7.11 及后面的注)

$$\frac{\phi-1}{n}\in \mathrm{End}_{F_q}(E). \tag{11.2}$$

若 $\phi\in\mathbb{Z}$, 式 (11.2) 等价于 $n|\phi-1$. 这时 $q=\phi\widehat{\phi}=\phi^2$, $t=\phi+\widehat{\phi}=2\phi$, 因而 $q+1-t=(\phi-1)^2$, 所以 $n|\phi-1$ 等价于 $n^2|q+1-t$. 因 $q-1=\phi^2-1$, 条件 $n|q-1$ 自然也成立.

若 $\phi\notin\mathbb{Z}$. 这时 $\mathbb{Q}(\phi)\subset\mathrm{End}_{F_q}(E)\otimes\mathbb{Q}\subset\mathrm{End}(E)\otimes\mathbb{Q}$, $\mathbb{Q}(\phi)$ 是 $\mathrm{End}_{F_q}(E)\otimes\mathbb{Q}$ 的中心, $\mathbb{Q}(\phi)$ 是虚二次域, 故 $\mathrm{End}_{F_q}(E)\otimes\mathbb{Q}=\mathbb{Q}(\phi)$, 所以$\mathrm{End}_{F_q}(E)$ 是 $\mathbb{Q}(\phi)$ 中的一个阶. 条件 (11.2) 等价于: $(\phi-1)/n$ 是 $\mathrm{End}_{F_q}(E)$ 中的代数整数. 计算 $\dfrac{\phi-1}{n}$ 的范数, 迹和 $\mathbb{Z}\left[\dfrac{\phi-1}{n}\right]$ 的判别式:

$$N\Big(\frac{\phi-1}{n}\Big)=\frac{\phi-1}{n}\cdot\frac{\widehat{\phi}-1}{n}=\frac{q+1-t}{n^2},$$

$$T\Big(\frac{\phi-1}{n}\Big)=\frac{\phi-1}{n}+\frac{\widehat{\phi}-1}{n}=\frac{t-2}{n}=\frac{q-1}{n}-\frac{q+1-t}{n},$$

$$\Delta\Big(\mathbb{Z}\Big[\frac{\phi-1}{n}\Big]\Big)=T\Big(\frac{\phi-1}{n}^2\Big)-4N\Big(\frac{\phi-1}{n}\Big)=\frac{t^2-4q}{n^2},$$

可见条件 (1) 与 (2) 等价, 证毕.

定理 11.4 $E(F_q)\cong\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}$, 且 $n_2|n_1,\ n_2|q-1$.

证明 设 m 为 $E(F_q)$ 中各点的阶的最小公倍数. 首先假设 m 与 q 互素, 一定存在 F_q 的某一扩域 F_{q^k}, 使 $E[m]\subset E(F_{q^k})$, $E[m]\cong\mathbb{Z}_m\oplus\mathbb{Z}_m$. $E(F_q)$ 是 $E[m]$ 的子群, 故 $E(F_q)\cong\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$, 利用交换群基本定理, 可得 $E(F_q)\cong\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}$, $n_2|n_1$. 这时由于 $E[n_2]\subset E(F_q)$, 故有 $n_2|q-1$(定理 11.3). 当 m 与 q 不互素时, 则有 $m=p^r\cdot m'$, m' 与 q 互素, 素数 $p|q$. 这时 $E(F_q)\cong\mathbb{Z}_{p^r}\oplus E(F_q)'$, $E(F_q)'$ 各元素的阶的最小公倍数即为 m', 它与 q 互素, 对 $E(F_q)'$ 应用上述已证的结果得到 $E(F_q)'\cong\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}$, 因而 $E(F_q)\cong\mathbb{Z}_{p^rn_1}\oplus\mathbb{Z}_{n_2}$, 证毕.

下面的定理 11.5 给出了当 E/F_q 为超奇异椭圆曲线时 $E(F_q)$ 的群结构.

定理 11.5 设 $t\in\mathbb{Z}$ 为 E/F_q 上的 q 阶 Frobenius 变换 ϕ 的迹, E/F_q 为超奇异.

(1) 若 $t^2=q,\ 2q$或$3q$, 则 $E(F_q)$ 为循环群.

(2) 若 $t^2=4q$, 当 $t=2\sqrt{q}$ 时, $E(F_q)\cong\mathbb{Z}_{\sqrt{q}-1}\oplus\mathbb{Z}_{\sqrt{q}-1}$; 当 $t=-2\sqrt{q}$ 时, $E(F_q)\cong\mathbb{Z}_{\sqrt{q}+1}\oplus\mathbb{Z}_{\sqrt{q}+1}$.

(3) 若 $t=0$, $q\not\equiv -1(\mathrm{mod}\ 4)$, 则 $E(F_q)$ 为循环群; 若 $t=0$, $q\equiv -1(\mathrm{mod}\ 4)$, 则 $E(F_q)$ 为循环群或 $E(F_q)\cong \mathbb{Z}_{(q+1)/2}\oplus\mathbb{Z}_2$.

证明 记 $t^2=\alpha q$, $\alpha=0,1,2,3,4$. 假设 $E[m]\subset E(F_q)$, 且 $E[m]\cong\mathbb{Z}_m\oplus\mathbb{Z}_m$, 这时 m 与 q 互素, 因而 $m^2|q+1-t$, $m|q-1$, 故 $q\equiv 1(\mathrm{mod}\ m)$, $t\equiv 2(\mathrm{mod}\ m)$. 由于 $(t-2)^2=\alpha q-4t+4\equiv\alpha-4(\mathrm{mod}\ m)$, 故 $m|4-\alpha$.

若 $\alpha=3$, 由于 $m|1$, 一定有 $m=1$; 若 $\alpha=2$, 这时 $m|2$ 且 m 与 2 互素, 故只能有 $m=1$; 若 $\alpha=1$, 这时 $m|3$, 由于 $q+1\pm\sqrt{q}$ 一定不是 9 的倍数, 所以 $m\neq 3$, 同样只能有 $m=1$, (1) 成立.

若 $\alpha=4$, 当 $t=2\sqrt{q}$ 时, ϕ 适合 $x^2-2\sqrt{q}+q=0$, 所以 $\phi=\sqrt{q}\in\mathbb{Z}$. 取 $m=\sqrt{q}-1$, 这时定理 11.3 的 (2) 成立, 由于 $\#E(F_q)=q+1-2\sqrt{q}=(\sqrt{q}-1)^2$, 所以 $E(F_q)\cong\mathbb{Z}_{\sqrt{q}-1}\oplus\mathbb{Z}_{\sqrt{q}-1}$. 类似地, 可以证明 $t=-2\sqrt{q}$ 时, $E(F_q)\cong\mathbb{Z}_{\sqrt{q}+1}\oplus\mathbb{Z}_{\sqrt{q}+1}$, (2) 成立.

若 $\alpha=0$, 这时 $m|4$, m 可能为 $1,2,4$. 当 $q\not\equiv -1(\mathrm{mod}\ 4)$ 时, 由 $m^2|q+1$ 可知 m 只能为 1; 当 $q\equiv -1(\mathrm{mod}\ 4)$ 时, 由 $m|q-1$ 可知 m 为 1 或 2, 于是 (3) 成立, 证毕.

设 E/F_q 为超奇异椭圆曲线, $E(F_q)=\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}$, $n_2|n_1$, n_1 和 n_2 由定理 11.5 所决定. 要完成式 (11.1) 中的步骤 (1), 实际上就是要找到最小的正整数 k, 使 $E[n_1]\subset E(F_{q^k})$, 因为 n 是 n_1 的因子, 这时自然有 $E[n]\subset E(F_{q^k})$. 依 $t^2=0,q,2q,3q,4q$ 的不同情况分别讨论. 当 $t^2=4q$ 时, 根据定理 11.5 的 (2), 显然有 $k=1$. 当 $t^2=q$ 时, $n_1=q+1\mp\sqrt{q}$, 因 $q^3-1=(q-1)(q+1+\sqrt{q})(q+1-\sqrt{q})$, 所以 $n_1|q^3-1$. E/F_{q^3} 上的 q^3 阶 Frobenius 变换 ϕ_{q^3}适合方程 $x^2\pm2\sqrt{q^3}x+q^3=0$(利用式 (7.21) 得 $V_3=\mp2\sqrt{q^3}$), 因而 $\phi_{p^3}=\pm\sqrt{q^3}\in\mathbb{Z}$. 由于 $q^3+1\pm2\sqrt{q^3}=(\sqrt{q}\pm1)^2(q+1\mp\sqrt{q})^2$, 可见 $n_1^2|q^3+1\pm2\sqrt{q^3}$, 所以 $E[n_1]\subset E(F_{q^3})$(定理 11.3(2)), 可取 $k=3$. 利用类似方法, 当 $t^2=2q$ 时, 可取 $k=4$; 当 $t^2=3q$ 时, 可取 $k=6$; 当 $t^2=0$ 时, 可取 $k=2$. 在上述所有情况下都有 $E(F_{q^k})\cong\mathbb{Z}_{cn_1}\oplus\mathbb{Z}_{cn_1}$, 其中 c 为正整数.

式 (11.1) 中的约化步骤 (2) 可如下进行. 任取 $Q'\in E(F_{q^k})$, 令 $Q=(cn_1/n)Q'$ ($\in E[n]$). 计算 $\alpha=e_n(P,Q)$, $\beta=e_n(D,Q)$, 在 F_{q^k} 中计算离散对数 l' 使 $\beta=\alpha^{l'}$. 若 $D=l'P$, 则计算完成. 否则, 说明 α 不是 n 次本原单位根, 改取另一 Q', 重复上述过程, 直到找到 l 使 $D=lP$. 找到 Q 使 α 为 n 次本原单位根的概率为 $\phi(n)/n$(ϕ 为 Euler 函数).

一个概率型算法, 如果它的计算时间的期望值以输入变量 x 的比特长度 (即 $\log x$) 的多项式为上界, 则称它为概率多项式算法. 如果该期望值以函数

$$L(\alpha,x)=\exp((c+o(1))(\log x)^{\alpha}(\log\log x)^{1-\alpha}),\quad 0<\alpha<1$$

为上界, 则称它为概率亚指数算法, 这里 $o(1)$ 表示无穷小量.

假设已有 F_q 在其素域 F_p 上的一组基, 随机取 $F_q[x]$ 中一 k 次不可约多项式 $f(x)$, 这是一个概率多项式算法 ($\log q$ 的多项式), 于是得到 $F_{q^k} \cong F_q[x]/(f(x))$. 当 $k \leqslant 6$ 时, 随机取 $Q' \in E(F_{q^k})$ 是一个概率多项式算法, 由 Q' 确定 Q 是多项式算法. 计算 Weil 对是多项式算法, 由于

$$\frac{n}{\phi(n)} \leqslant b \log\log n, \quad n \geqslant 5,$$

以及 $n = O(q)$, 通过 $O(\log\log q)$ 次迭代可以找到 Q, 使 $e_n(P,Q)$ 为 n 次本原单位根. 检查 $D = l'P$ 是否成立是多项式算法. 综合上述, 将超奇异椭圆曲线上的 ECDLP 化为 F_{q^k} 上的 DLP 是概率多项式算法. 关于有限域上的离散对数计算, 当 p 固定, $k \to \infty$ 时, 已有计算 F_{q^k} 上的离散对数的概率亚指数算法 (见 11.7 节). 综合上述, 对于超奇异椭圆曲线上的 ECDLP 有概率亚指数算法. 在构造椭圆曲线公钥密码时, 将不采用超奇异椭圆曲线.

11.5 FR 约化

Frey, Müller 和 Rück 利用 Tate 对给出一个方法[17], 在一定条件下 $(n|q-1)$, 将 F_q 曲线的除子类群中离散对数的计算化为 F_q^* 中离散对数的计算. 由于椭圆曲线与除子类群 $\mathrm{Pic}^\circ(E)$ 是同构的, 在本节中, 将 FR 约化应用于椭圆曲线[16].

首先, 简单介绍群的上同调.

设 G 为有限群, M 为交换群, G 中元素可作用在 M 上. 将 $\delta \in G$ 在 $m \in M$ 上的作用记为 $m \mapsto m^\delta$, 并假定它满足条件:

$$m^1 = m, \quad (m+m')^\delta = m^\delta + {m'}^\delta, \quad (m^\delta)^\tau = m^{\delta\tau},$$

其中 1 为 G 的单位, 这时称 M 为 G 模. 设 M 和 N 为两个 G 模, $\phi\colon\ M \to N$ 为同态, 且适合

$$\phi(m)^\delta = \phi(m^\delta), \quad \forall m \in M, \quad \delta \in G,$$

称 ϕ 为 G 同态.

定义 11.1 G 模 M 的零阶上同调群为

$$H^0(G,M) = \{m \in M \,|\, m = m^\delta,\ \forall \delta \in G\},$$

即 $H^0(G,M)$ 为 M 中由 G 不变元素组成的子模, 有时也记作 M^G.

设

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

是 G 模正合序列 (即序列中前一 G 同态的像是后一 G 同态的核), 可见 ϕ 是单射, ψ 是满射, 且 ϕ 的像为 ψ 的核. 在每个 G 模中取 G 不变量, 得到 G 模正合序列

$$0 \longrightarrow P^G \xrightarrow{\phi} M^G \xrightarrow{\psi} N^G,$$

最右端的 G 同态就不一定是映上的, 为了研究它的像集, 引入下述定义.

定义 11.2　设 M 为 G 模, 令

$$C^1(G,M) = \{\xi : G \to M\}$$

为由 G 到 M 的所有映射 (也称 1-链) 组成的 (加法) 群, 令

$$Z^1(G,M) = \{\, \xi \in C^1(G,M) \,|\, \xi_{\delta\tau} = \xi_\delta^\tau + \xi_\tau,\ \forall \delta, \tau \in G\,\}$$

为由 G 到 M 的 1-闭上链组成的群, 令

$$\mathcal{B}^1(G,M) = \{\, \xi \in C^1(G,M) \,|\, 存在 m \in M, 使\ \xi_\delta = m^\delta - m,\ \forall \delta \in G\,\}$$

为由 G 到 M 的 1-上边缘组成的群. 显然 $\mathcal{B}^1(G, M) \subset Z^1(G, M)$. G 模 M 的 1 阶上同调群 $H^1(G, M)$ 定义为

$$H^1(G,M) = Z^1(G,M)/\mathcal{B}^1(G,M),$$

两个 1-闭上链之差若为 1-上边缘, 它们对应 $H^1(G,M)$ 中同一上同调类.

设 $\phi : M \to N$ 为 G 同态, 则 ϕ 将 $Z^1(G, M)$ 中映射到 $Z^1(G, N)$, 将 $\mathcal{B}^1(G, M)$ 映射到 $\mathcal{B}^1(G, N)$, 所以 ϕ 诱导映射 $H^1(G,M) \to H^1(G,N)$.

定理 11.6　设

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

是 G 模正合序列, 则有正合序列

$$\begin{aligned} 0 \longrightarrow & H^0(G,P) \longrightarrow H^0(G,M) \longrightarrow H^0(G,N) \\ \xrightarrow{\delta} & H^1(G,P) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N), \end{aligned}$$

其中 δ 定义为:

对任一 $n \in H^0(G,N)$, 取 $m \in M$, 使 $\psi(m) = n$, 定义 1-闭上链 $\xi \in Z^1(G,P)$:

$$\xi_\delta = m^\delta - m, \quad \forall \delta \in G,$$

$\delta(n)$ 即为 ξ 在 $H^1(G,P)$ 中所属的上同调类.

证明 因 $n \in N^G$, 故 $\psi(\xi_\delta) = \psi(m)^\delta - \psi(m) = n^\delta - n = 0$, 所以 $\xi_\delta \in \text{Ker}\psi = \text{IM}(\phi) \cong P$, 可以认为 ξ_δ 属于 P, 即 $\xi \in H^1(G, P)$. 易见 ξ 所在的上同调类不依赖于 m 的选择. 证明的其余部分虽然比较烦琐, 但都是可以根据定义直接推出的.

将定理 11.6 应用于椭圆曲线, 设 E'/F_q, E/F_q 为椭圆曲线, ϕ 为定义在 F_q 上的同种映射 $E' \to E$. 取 $G = \text{Gal}(\overline{F}_q/F_q)$, 有 G 模正合序列

$$0 \longrightarrow E'[\phi] \longrightarrow E'(\overline{F}_q) \xrightarrow{\phi} E(\overline{F}_q) \longrightarrow 0,$$

$E'[\phi]$ 表示 ϕ 的核. 利用定理 11.6, 得到正合序列

$$\begin{aligned} 0 \longrightarrow E'(F_q)[\phi] \longrightarrow E'(F_q) \xrightarrow{\phi} E(F_q) \\ \xrightarrow{\delta_E} H^1(G, E'[\phi]) \longrightarrow H^1(G, E'(\overline{K}_q)). \end{aligned}$$

可见有正合序列

$$0 \longrightarrow E(F_q)/\phi(E'(F_q)) \xrightarrow{\delta_E} H^1(G, E'[\phi]) \xrightarrow{\phi} H^1(G, E'(\overline{K}_q))[\phi] \longrightarrow 0,$$

其中

$$\begin{aligned} \delta_E : E(F_q)/\phi(E'(F_q)) &\longrightarrow H^1(G, E'[\phi]) \\ P \longmapsto \quad & \delta \longmapsto Q^\delta - Q, \end{aligned}$$

这里 $P \in E(F_q)$, $Q \in E'(\overline{F}_q)$, $\phi(Q) = P$.

设 n 为正整数, n 与 q 互素, 考虑乘法群 $\overline{F}_q^*$ 中 n 次幂运算, 得 G 模正合序列

$$1 \longrightarrow \mu_n \longrightarrow \overline{F}_q^* \longrightarrow \overline{F}_q^* \longrightarrow 1.$$

假设 $\mu_n \subset F_q$, 即 $n|q-1$, 利用定理 11.6 可得到正合序列

$$1 \longrightarrow \mu_n \longrightarrow F_q^* \xrightarrow{n} F_q^* \xrightarrow{\delta_F} H^1(G, \mu_n) \longrightarrow H^1(G, \overline{F}_q^*).$$

由于 $H^1(G, \overline{F}_q^*) = 1$ (Hilbert 定理 90), 可得正合序列

$$1 \longrightarrow F_q^*/(F_q^*)^n \xrightarrow{\delta_E} H^1(G, \mu_n) \longrightarrow 1,$$

其中

$$\begin{aligned} \delta_F : F_q^*/(F_q^*)^n &\longrightarrow H^1(G, \mu_n) \\ b \longmapsto \quad & \delta \mapsto \beta^\delta/\beta \end{aligned}$$

是一个同构, 这里 $\beta \in \overline{F}_q^*$, 且 $\beta^n = b$.

特别地, 取 $E' = E$, $\phi = [n]$, 利用 Weil 对 $e_n : E[n] \times E[n] \longrightarrow \mu_n$ 定义 Tate 对:

$$\begin{aligned} b : E(F_q)/n(E(F_q)) \times E(F_q)[n] &\longrightarrow F_q^*/(F_q^*)^n \\ (P, T) \longmapsto \quad & \delta_F^{-1}\big(e_n(\delta_E(P), T)\big). \end{aligned}$$

这里 $e_n(\delta_E(P),T) \in H^1(G,\mu_n)$, $e_n(\delta_E(P)(\delta),T) = \beta^\delta/\beta$ $(\forall\ \delta \in G)$, 其中 $\beta^n = b(P,T)$.

由 Weil 对的双线性, 不难推出 $b(P,T)$ 的双线性. 可以证明 $b(P,T)$ 是非退化的[32]. $b(P,T)$ 可用以下的方法计算. 由于 $T \in E(F_q)[n]$, 可找到函数 f_T, $g_T \in F_q(E)$, 使

$$\mathrm{div}(f_T) = n(T) - n(\mathcal{O}), \quad f_T \circ [n] = g_T^n.$$

因而

$$e_n(\delta_E(P)(\delta),T) = e_n(Q^\delta - Q,T) = g_T(X + Q^\delta - Q)/g_T(X),$$

取 $X = Q$, 由于 $g_T \in F_q(E)$, 故得

$$g_T(Q^\delta)/g_T(Q) = g_T(Q)^\delta/g_T(Q),$$

所以当 $P \neq T$ 时,

$$b(P,T) = g_T(Q)^n = f_T \cdot [n](Q) = f_T(P)(\mathrm{mod}\ F_q^{*n}).$$

当 $P = T$ 时, 任取 $P_1 \in E(F_q)$ 使 $P + P_1$, $P_1 \notin R(n)$(定义见 11.4 节), 利用 b 的双线性得到

$$b(T,T) \equiv f_T(T + P_1) \cdot f_T(P_1)^{-1}\ (\mathrm{mod}\ F_q^{*n}).$$

当 $n|q-1$ 时, 有同构映射

$$\begin{aligned}\gamma : F_q^*/(F_q^*)^n &\longrightarrow \mu_n\\ a &\longmapsto a^{\frac{q-1}{n}}.\end{aligned}$$

将 b 与 γ 复合, 得到 Tate-Lichtenbaum 对

$$\begin{aligned}\Phi_m : E(F_q)/n(E(F_q)) \times E(F_q)[n] &\longrightarrow \mu_n\\ (P,T) &\longmapsto \big(b(P,T)\big)^{\frac{q-1}{n}}.\end{aligned}$$

注 1 f_T 的选取可以相差一个常数因子, 但由于 $f_T \circ [n] = g_T^n$, 故该常数因子属于 F_q^{*n}, 即在 $\mathrm{mod}\ F_q^{*n}$ 的意义下, f_T 是唯一的.

注 2 对于 Weil 对, 一定有 $e_n(T,T) = 1$. 但对于 Tate-Lichtenbaum 对, $\Phi_m(T, T)$ 不一定是 1, 它将在离散对数的计算中发挥重要作用.

设 $T \in E(F_q)[n]$, $P \in \langle T\rangle$, n 为素数, $n|q-1$. 利用 Tate-Lichtenbaum 对可将 E 上的离散对数计算化为 F_q^* 上的离散对数计算. 计算 $\alpha = \Phi_n(T,T)$, $\beta = \Phi_n(T,p)$. 若 α 为 n 次本原单位根, 在 F_q^* 上计算离散对数 m, 使 $\beta = \alpha^m$, 就可得到 $P = mT$. 由于 n 为素数, α 为 n 次本原单位根 (即 $\alpha \neq 1$) 的概率为 $1 - \dfrac{1}{n}$.

在利用 MOV 约化时, 首先要求找到 k, 使 $E[n] \subset E(F_{q^k})$, 然后将 E 上的离散对数的计算化为 $F_{q^k}^*$ 上离散对数的计算. 在使用 FR 约化时, 仅要求 $n|q-1$, 并不要求 $E[n] \subset E(F_q)$, 所以 FR 约化可以在 $E[n] \not\subset E(F_q)$ 的情况下使用. 由于 $n|\#E(F_q) = q+1-t$, 所以 $t \equiv 2 \pmod{n}$, t 为 F_q 上 q 阶 Frobenius 变换的迹.

当 n 为素数, $n \nmid q$, $n \nmid q-1$ 时, 条件 $E[n] \subset E(F_{q^k})$ 等价于条件 $n|q^k-1$[2], 这时使用 MOV 约化和使用 FR 约化要求的条件是相同的.

11.6 SSSA 约化

在 FR 约化和 MOV 约化中, 循环群 $\langle P\rangle$ 同构嵌入 F_q(或其扩域 F_{q^k}) 的乘法群中, 从而将 $\langle P\rangle$ 上离散对数的计算化为 F_q^*(或 $F_{q^k}^*$) 上离散对数的计算. 本节介绍 Smart-Semaev-Satoh-Araki 提出的计算 ECDLP 的方法[45,48,50], 它将群 $\langle P\rangle$ 同构嵌入 F_q^+ (F_q 的加法群), 从而将 $\langle P\rangle$ 上离散对数的计算化为 F_q^+ 上离散对数的计算.

设 $q=p^m$, $p \neq 2,3$ 为素数, E/F_q 由方程 $y^2 = x^3+ax+b$ 定义, $P \in E(F_q)$ 的阶为 p. 这类曲线称为异常 (anomalous) 椭圆曲线, 当 $q=p$ 时, 异常曲线上的 p 阶 Frobenius 变换的迹 $t=1$.

任一点 $Q=(x_Q,y_Q) \in E(F_q)$, 当 D 不是二阶点和无穷远点时, Q 的单值化子 $t_Q = x-x_Q$; 当 $Q=(x_Q,0)$ 为二阶点时, $t_Q=y$; 当 $Q=\mathcal{O}$ 时, $t_Q=x/y$.

引理 11.2 设 $f \in \overline{F}_q(E)$, $\mathrm{div}(f)=pD$, D 不是主除子. 令 $f'=\mathrm{d}f/\mathrm{d}x$, 则

$$\mathrm{div}(f') = \mathrm{div}(f) - \mathrm{div}(y).$$

证明 当 D 不是主除子时, f' 不恒为零. 设 $D=\sum n_Q(Q)$, 则 $f=t_Q^{pn_Q}f_1$, $\mathrm{ord}_Q(f_1)=0$. 当 Q 不是二阶点和无穷远点时, $\mathrm{d}f/\mathrm{d}x = \mathrm{d}f/\mathrm{d}t_Q = t_Q^{pn_Q}\mathrm{d}f_1/\mathrm{d}t_Q$, 从而 $\mathrm{ord}_Q(f') = pn_Q + m_Q$, 其中 $m_Q = \mathrm{ord}_Q(\mathrm{d}f_1/\mathrm{d}t_Q) \geqslant 0$. 当 Q 为二阶点时,

$$\mathrm{d}f/\mathrm{d}x = \mathrm{d}f/\mathrm{d}y \cdot \mathrm{d}y/\mathrm{d}x = y^{pn_Q}\Big((3x^2+a)/2y\Big)\mathrm{d}f_1/\mathrm{d}y,$$

因 $\mathrm{ord}_Q\big((3x^2+a)/2y\big)=-1$, 故 $\mathrm{ord}_Q(f')=pn_Q-1+m_Q$, 其中 $m_Q=\mathrm{ord}_Q(\mathrm{d}f_1/\mathrm{d}y) \geqslant 0$; 当 $Q=\mathcal{O}$ 时,

$$\mathrm{d}f/\mathrm{d}x = \mathrm{d}f/\mathrm{d}(x/y) \cdot \mathrm{d}(x/y)/\mathrm{d}x = (x/y)^{pn_Q}\big((-x^3+ax+2b)/2y^3\big) \cdot \mathrm{d}f_1/\mathrm{d}(x/y).$$

由于 $\mathrm{ord}\big((-x^3+ax+2b)/2y^3\big) = 3$, 故 $\mathrm{ord}_Q(f') = pn_Q+3+m_Q$, 其中 $m_Q = \mathrm{ord}_Q(\mathrm{d}f_1/\mathrm{d}(x/y)) \geqslant 0$, 则有

$$\mathrm{div}(y) = (S_1)+(S_2)+(S_3)-3(\mathcal{O}),$$

其中 S_1, S_2, S_3 为 E 上三个二阶点, 故 $\mathrm{div}(f') = \mathrm{div}(f) - \mathrm{div}(y) + D_1$, 其中 $D_1 = \sum m_Q(Q)$, 可见 D_1 是主除子, 所有的 m_Q 均为零, 证毕.

取一固定点 $R \in \langle P \rangle$, $R \neq Q$. 对任一 $Q \in \langle P \rangle$, 存在函数 $f_Q \in F_q(E)$, 使 $\mathrm{div}(f_Q) = p(Q) - p(\mathcal{O})$. 定义映射

$$\begin{aligned}\Phi : \langle P \rangle &\longrightarrow F_q^+\\ Q &\longmapsto (f_Q'/f_Q)(R), Q \neq \mathcal{O}\\ \mathcal{O} &\longmapsto 0.\end{aligned}$$

定理 11.7 $\Phi(Q)$ 的定义是有意义的, Φ 是 $\langle P \rangle$ 到 F_Q^+ 的同构嵌入.

证明 从引理 11.2 得到 $\mathrm{div}(f_Q'/f_Q) = -\mathrm{div}(y)$, R 不是二阶点和无穷远点, 所以 $\Phi(Q)$ 是 F_q^+ 中的非零元, 仅需证 Φ 是同态映射.

设除子 D' 与 $D = (Q) - (\mathcal{O})$ 线性等价, 则存在函数 g, 使 $\mathrm{div}(g) = D - D'$, 若 $\mathrm{div}(f) = pD'$, 易见 $f_Q = f \cdot g^p$, 这时 $f'/f = f_Q'/f_Q$. 在定义 $\Phi(Q)$ 时可以任取一个与 D 线性等价的除子代替 D. 设 $Q_i \in \langle P \rangle$, $D_i = (Q_i) - (\mathcal{O})$, $\mathrm{div}(f_{Q_i}) = pD_i$, $i = 1, 2$. 令 $D_{Q_1+Q_2} = D_1 + D_2 = (Q_1) + (Q_2) - 2(\mathcal{O}) \sim (Q_1 + Q_2) - (\mathcal{O})$, 取函数 $f_{Q_1+Q_2}$, 使 $\mathrm{div}(f_{Q_1+Q_2}) = pD_{Q_1+Q_2} = \mathrm{div}(f_{Q_1} \cdot f_{Q_2})$, $f_{Q_1+Q_2}$ 与 $f_{Q_1} \cdot f_{Q_2}$ 仅差一个常数因子, 故

$$f_{Q_1+Q_2}'/f_{Q_1+Q_2} = f_{Q_1}'/f_{Q_1} + f_{Q_2}'/f_{Q_2}.$$

Φ 是同态映射, 证毕.

考虑如何计算$\Phi(Q)$. 取二阶点S, 存在函数 f_Q, 使 $\mathrm{div}(f_Q) = p(Q+S) - p(S) \sim p(Q) - p(\mathcal{O})$. 由上述可知 $\Phi(Q) = (f_Q'/f_Q)(R)$. 在 $\langle P \rangle \times F_q^+$ 上定义一个运算

$$(Q_1, a_1) \oplus (Q_2, a_2) = (Q_1 + Q_2, a_1 + a_2 + (h'/h)(R)),$$

其中函数 h 适合

$$\begin{aligned}\mathrm{div}(h) =&(Q_1 + S) + (Q_2 + S) - (Q_1 + Q_2 + S) - (S)\\ =&\{(Q_1 + S) + (Q_2 + S) + (-Q_1 - Q_2 + S) - 3(S)\}\\ &- \{(Q_1 + Q_2 + S) + (-Q_1 - Q_2 + S) - 2(S)\}\\ =&\mathrm{div}(\lambda_{Q_1,Q_2}) - \mathrm{div}(\eta_{Q_1+Q_2}).\end{aligned}$$

函数$\lambda_{Q_1,Q_2}(X+S)$和$\eta_{Q_1+Q_2}(X+S)$ 都是x, y 的线性函数, 前者是通过$Q_1, Q_2, -(Q_1+Q_2)$ 的直线, 后者是通过 $Q_1 + Q_2, -(Q_1 + Q_2)$ 的直线, 则有

$$h'/h = \lambda_{Q_1,Q_2}'/\lambda_{Q_1,Q_2} - \eta_{Q_1+Q_2}'/\eta_{Q_1+Q_2}.$$

等式右端的二项可用下述方法计算, 设 $\delta(X) = Ax + By + C$ $(A, B, C \in F_q)$ 是上述提及的直线, 令 $\delta_1(X) = \delta(X - S)$, 欲计算 δ_1'/δ_1, 易见

$$\delta' = A + B\mathrm{d}y/\mathrm{d}x = A + B(3x^2 + A)/2y$$

及 $\mathrm{d}\delta = 2y\delta'\mathrm{d}x/2y$, 通过直接计算可以发现 $\mathrm{d}x/2y(X - S) = \mathrm{d}x/2y$(实际上, $\mathrm{d}x/2y$ 在任一平移变换下不变, 见文献 [49], 第三章命题 5.1), 所以

$$\mathrm{d}\delta(X - S) = (2y\delta')(X - S)(\mathrm{d}x/2y)(X - S) = (2y\delta')(X - S) \cdot \mathrm{d}x/2y,$$

故

$$(\delta_1'/\delta_1)(X) = \mathrm{d}\delta(X - S)/\mathrm{d}x \cdot \delta(X - S)^{-1} = (2y\delta')(X - S)/2y\delta(X - S). \quad (11.3)$$

当以 $X = R$ 代入时, $R - S$ 不是二阶点和无穷远点, 上式右端为 F_q^+ 中的非零元.

设 $p = \alpha_0 + 2\alpha_1 + \cdots + 2^t\alpha_t$ $(\alpha_i = 0, 1)$, 从 $(Q, 0)$ 出发, 依次计算 $(2Q, a_1), \cdots, (2^tQ, a_t)$, 然后计算 $\alpha_0(Q, 0) \oplus \alpha_1(2Q, a_1) \oplus \cdots \oplus \alpha_t(2^tQ, a_t) = (\mathcal{O}, (f_Q'/f_Q)(R))$. 可见 $\Phi(Q)$ 的计算量为 $O(\log p)$.

若 $Q \in \langle P \rangle$, $Q = lP$, 则由 $\Phi(Q) = l\Phi(P)$ 可得 $l = \Phi(Q) \cdot \Phi(P)^{-1}$.

实际上, 为了通过式 (11.3) 计算 $\Phi(Q)$, 可取 E 上任一不在 $\langle P \rangle$ 中的点代替 S. 但由于二阶点 $S = (\alpha, 0)$, α 适合方程 $x^3 + ax + b = 0$, 所以 $F_Q(\alpha)$ 最多为 F_q 的三次扩张, 选用二阶点时上述所有计算可以在 F_{q^3} 中完成.

文献 [52] 给出了异常曲线上 DLP 的另一种算法, 它可以保证所有的计算在 F_q 中完成. 取 $R = \mathcal{O}$, 对任一 $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, 取函数 $f_Q \in F_q(E)$, 使

$$\mathrm{div}(f_Q) = p(Q + P) - p(P). \quad (11.4)$$

定义映射

$$\begin{aligned} \Psi : \langle P \rangle &\longrightarrow F_q^+ \\ Q &\longmapsto \Big(\frac{\mathrm{d}f_Q/\mathrm{d}t}{f_Q}\Big)(\mathcal{O}),\ Q \neq \mathcal{O} \\ \mathcal{O} &\longmapsto 0, \end{aligned}$$

其中 $t = x/y$ 为 $\mathcal{O}$ 的单值化子 (注意: 这里用 $\mathrm{d}f_Q/\mathrm{d}t$ 代替 $\mathrm{d}f_Q/\mathrm{d}x$), f_Q 在 $\mathcal{O}$ 处有展开式

$$f_Q = \begin{cases} a_0 + a_1t + O(t^2), & Q \neq -P, \\ t^p\big(b_0 + b_1t + O(t^2)\big), & Q = -P. \end{cases}$$

由式 (6.2), 可知 $a_0 \neq 0$, $b_0 \neq 0$, 易见,

$$\Psi(Q) = \begin{cases} a_1/a_0, & Q \neq -P, \\ b_1/b_0, & Q = -P. \end{cases}$$

类似于定理 11.7, 可以证明 Ψ 是 $\langle P\rangle$ 到 F_q^+ 的同态, 由引理 11.2,

$$\begin{aligned}\mathrm{ord}_{\mathcal{O}}(\mathrm{d}f_P/\mathrm{d}t) &= \mathrm{ord}_{\mathcal{O}}(\mathrm{d}f_P/\mathrm{d}x) - \mathrm{ord}_{\mathcal{O}}(\mathrm{d}t/\mathrm{d}x)\\ &= \mathrm{ord}_{\mathcal{O}}(f_P) - \mathrm{ord}_{\mathcal{O}}(y) - \mathrm{ord}_{\mathcal{O}}(\mathrm{d}t/\mathrm{d}x)\\ &= \mathrm{ord}_{\mathcal{O}}(f_P) \neq 0\end{aligned}$$

(这里利用了 $\mathrm{ord}_{\mathcal{O}}(y) = -\mathrm{ord}_{\mathcal{O}}(\mathrm{d}t/\mathrm{d}x) = 3$), 可见, $\Psi(P)\neq 0$, Ψ 是 $\langle P\rangle$ 到 F_q^+ 的同构嵌入. 也可以得到与计算 $\Phi(Q)$ 类似的计算 $\Psi(Q)$ 的算法.

11.7 有限域上离散对数的计算

MOV 约化和 FR 约化, 将计算 F_q 上的椭圆曲线离散对数化为计算有限域乘法群 $F_{p^k}^*$ 上的离散对数, 这里约定 $p\neq 2,3$ 为一个素数. 本节介绍计算 $F_{p^k}^*$ 上的离散对数的指标计算法 (index calculus method), 并证明它是一个亚指数算法.

首先介绍一般的 n 阶循环群 G 上的指标计算法. 设 g 为 G 的生成元, $p_1,\cdots,p_m$ 为 G 中 m 个元素. 算法的第一步是设法找到足够多的关系式

$$\prod_{j=1}^{m} p_j^{a_{ij}} = g^{b_i}, \tag{11.5}$$

由此得到一组线性同余式

$$\sum_{j=1}^{m} a_{ij}\mathrm{ind}_g p_j = b_i \,(\mathrm{mod}\ n). \tag{11.6}$$

假定从这组同余式可以解得 $\mathrm{ind}_g p_j$ $(1\leqslant j\leqslant m)$, 算法的第二步是解这组同余式. 设 a 为 G 中任一元素, 算法的第三步是计算 $\mathrm{ind}_g a$. 设法找到一个正整数 e, 使得

$$\prod_{j=1}^{m} p_j^{e_j} = ag^e,$$

由此可得到 $\mathrm{ind}_g a = \sum\limits_{j=1}^{m} e_j\,\mathrm{ind}_g p_j - e$. 算法的前两步是预运算. 当要计算某一元素的离散对数时, 仅需要进行第三步. 第三步所需要的时间比前两步要少得多.

对于一般群 G, 指标计算法并不一定是可行的, 因为不一定能找到足够多的关系式 (11.5). 该方法在 $F_{p^k}^*$ 上是可行的, 本节将介绍 $F_{p^k}^*$ 上的指标计算法, 估计它需要做多少次 F_{p^k} 上的运算, 证明它是一个亚指数算法.

首先考虑 $k=1$ 的情况, 即 F_p^* 上的指标算法. 设 $p_1,p_2,\cdots,p_m$ $(<p)$ 为最小的 m 个素数. 算法的第一步是寻找关系式 (11.5), 随机取整数 $b\in[1,p-1]$, 计算最

小的正整数 r, 使 $r \equiv g^b (\bmod\ p)$, 这里 g 是模 p 的原根. 用 $p_1, \cdots, p_m$ 依次试除 r, 如果 r 是这 m 个素数的乘积, 则找到一个所要的关系式. 这时称 r 是一个光滑数, 或称 r 是 ρ_m-光滑的. 找到一个光滑数就找到一个关系式 (11.5).

显然, m 越大, r 为光滑数的机会就越大, 在算法的第一步找出足够的光滑数所需的计算量就会减少. 但在算法的第二步, 求解关于 $\mathrm{ind}_g p_i$ 的线性方程组的计算量就会增加, 证明 r 是光滑数的计算量也会增加. 因此需要选取适当的 m, 优化所需的总的计算量.

设 x, y 为正整数, 令

$$\varphi(x,y) = \#\{a \in \mathbb{Z} | 1 \leqslant a \leqslant x,\ a\text{的所有素因子不超过}y\},$$

则随机取 b, 使相应的 r 为光滑数的概率为

$$\varphi(p, p_m)/p.$$

由文献 [7] 的结果知

$$\varphi(x,y) = x \exp\big((-1+o(1))\mu \log \mu\big),$$

其中 $\mu = \log x / \log y$, $\mu \to \infty$ 及 $y \geqslant \log^2 x$. 令

$$L(p) = \exp\big(\sqrt{\log p \log\log p}\big),$$

取 $p_m \approx L(p)^c$, 这里 c 为一常数, 由素数定理可见,

$$m \approx p_m / \log p_m = L(p)^{c+o(1)}, \quad \log p / \log p_m = c^{-1}\sqrt{\log p / \log\log p},$$

因而

$$\begin{aligned}&\varphi(p,p_m)/p\\ =&\exp\big((-1+o(1)) \cdot c^{-1}\sqrt{\log p/\log\log p}(2^{-1}\log\log p - 2^{-1}\log(\log\log p) - \log c)\big)\\ =&L(p)^{-1/2c+o(1)}.\end{aligned}$$

所以平均随机选取 $L(p)^{1/2c+o(1)}$ 个 b 后, 可以得到一个式 (11.5) 的关系式, 欲得 $2m$ 个关系式, 需选取

$$2mL(p)^{1/2c+o(1)} = L(p)^{c+1/2c+o(1)}$$

个 b 值. 当 b 值选定后, 最多做 $m + \log p$ 次试除, 可以确定相应的 r 是否是光滑数 $\left(\text{若}r = \prod\limits_{i=1}^{m} p_i^{a_i}, \text{则} \sum\limits_{i=1}^{m} a_i \leqslant \log r < \log p\right)$. 所以指标计算法第一步的计算量为

$L(p)^{2c+1/2c+o(1)}$ 次 F_p 中的运算.

假定得到 $2m$ 个式 (11.5) 中的关系式后, 通过求解线性同余方程组 (11.6), 可以得到 $\mathrm{ind}_g p_i$ $(1 \leqslant i \leqslant m)$, 这假定看来是合理的, 但不可能严格证明. 在求解线性同余方程组时, 需要利用中国剩余定理将模 $p-1$ 的方程组化为模 $p-1$ 素因子 q 的方程组. 利用 Gauss 消去法求解素域 F_q 上 m 阶线性方程组的计算量为 $O(m^3)$. 在得到 F_q 上的解后, 可以进一步得到模素数幂 q^l(这里 $q^l \| p-1$) 的解 (参阅定理 2.16 的证明, 将类似方法应用于线性同余方程组, 文献上将这方法称为 Hensel 方法, 参见附录 A.4). 因此指标计算法的第二步所需计算量为 $O\big(L(p)^{3c+o(1)}\big)$.

设 $a \in F_p^*$, 在算法的第三步计算 $\mathrm{ind}_g a$, 任取整数 e, 使 $r \equiv ag^e \pmod p$ 为光滑数. 利用上述第一步中所作的分析, 可知第三步的计算量为 $O\big(L(p)^{c+1/2c+o(1)}\big)$.

若取 $c = 1/2$, 由上述分析, 可见 F_p^* 上指标计算法的计算量为 $O\big(L(p)^{2+o(1)}\big)$, 当 $p \to \infty$ 时, 它是一个亚指数算法.

现在考虑 $F_{p^k}^*$ 上的指标计算法. 将证明当 p 固定, $k \to \infty$ 时该算法是一个亚指数算法 (参阅文献 [22]).

设 g 为 $F_{p^k}^*$ 的生成元, 则 $g' = g^{(p^k-1)/(p-1)}$ 是 F_p^* 的生成元. 假定已知 F_p^* 中任一元素以 g' 为基的对数, 例如, 这可由上述 F_p^* 上的指标计算法得到. 把 F_p 中的元素称为纯量元. $F_{p^k}^*$ 中任一元素都可唯一地用 F_p 上的一个次数小于 k 的多项式表示, 设 $m < k$ 为正整数 (其数值将在下面确定), 以 S_m 表示 F_p 上的所有次数大于零且不超过 m 的首一不可约多项式的集合, $P(m)$ 表示 S_m 中多项式的个数. 在指标计算法中, 这组多项式将具有上述 F_p 的情况下, 最初的 m 个素数 $p_1, \cdots, p_m$ 同样的作用.

定义 11.3 *F_p 上的一个多项式若能分解为一个纯量元和若干个次数不超过 m 的首一不可约多项式之乘积, 则称该多项式 (相对 m) 是光滑的. $F_{p^k}^*$ 中的一个元素若可用光滑多项式表示, 则称该元素是光滑的.*

$F_{p^k}^*$ 上指标计算法的第一步是要找到 $F_{p^k}^*$ 中足够多的光滑元. 设

$$\alpha = g^b = cR$$

是一个光滑元, R 是 F_p 上的一个首一多项式, 现在把 R 也理解为一个 $P(m)$ 维向量, 其分量为 R 的因子分解式中对应 S_m 中每个不可约因子的指数, 纯量 c 的对数, 当 p 较小时, 可用列表法给出, 当 p 很大时, 如上所述, 可用 F_p^* 上的指标计算法得到.

引理 11.3 *F_{p^k} 中相对 m 的光滑元至少有 $\dbinom{P(m)+u}{u}$ 个, 其中 $u = \left[\dfrac{k-1}{m}\right]$.*

证明 在 S_m 中任取 u 个或少于 u 个不可约多项式, 它们的乘积的次数不超过 $u \cdot m \leqslant k-1$, 因而对应 F_{p^k} 中的一个光滑元. 如果在集合 S_m 中添加一个元素

"1", 则在 $S_m \cup \{1\}$ 中任取 u 个元素 (可以重复取同一元素), 每次都得到一个不同的光滑元, 如此取法的个数为函数

$$f(x) = (1-x)^{-(P(m)+1)}$$

关于 x 的展开式中 x^u 项的系数, 即为

$$\frac{1}{u!} \cdot \frac{\mathrm{d}^u}{\mathrm{d}x^u} f(x)\Big|_{x=0} = \frac{(P(m)+1)(P(m)+2)\cdots(P(m)+u)}{u!} = \binom{P(m)+u}{u},$$

证毕.

引理 11.4 当 $m \geqslant 1$ 时, $\dfrac{p^m}{2m} \leqslant P(m) \leqslant p^{m+1}$.

证明 后一不等式是显然的, 因为 m 次多项式共有 p^{m+1} 个. 以 $I(i)$ 表示 i 次首一不可约多项式的个数, 则

$$P(m) = \sum_{i=1}^{m} I(i) \geqslant I(m).$$

Berlekamp 在文献 [3] 中证明了

$$I(m) \geqslant \frac{p^m}{m}\big(1 - p^{1-m/2}\big),$$

所以当 $m \geqslant 4$ 时, 有

$$I(m) \geqslant \frac{p^m}{m}\Big(\frac{1}{2}\Big),$$

即证明了引理中的前一个不等式. 还需考虑 $m = 1, 2, 3$ 的情况, 利用公式

$$I(m) = \frac{1}{m} \sum_{d|m} \mu(d) p^{m/d}$$

(见文献 [33] 定理 3.25) 得

$$I(1) = p, \quad I(2) = \frac{1}{2}(p^2 - p) \geqslant \frac{p^2}{4}, \quad I(3) = \frac{1}{3}(p^3 - p) \geqslant \frac{p^3}{6},$$

引理证毕.

从算法第一步得到一组光滑元 R_i $(1 \leqslant i \leqslant I)$, 如何保证能在第二步从线性同余方程组 (11.6) 解出 $\mathrm{ind}_g f$ $(f \in S_m)$, 这是一个较困难的问题, 为此, 引入下述定义将有助于达到上述目的.

定义 11.4 随机生成的向量组 $\{R_i\}$, $1 \leqslant i \leqslant I$ 称为事实上的支架集合, 如果再按同样的随机方式生成任一向量 R, R 可表为 $\{R_i\}$ 的 (整系数) 组合的概率大于 $1/2$.

令 $l = k \cdot \ln p$, 这里 $\ln p$ 是以 2 为底的对数, l 是表示 F_{p^k} 中每一元素所需的比特长度. 令

$$m = \left[\frac{1}{\ln p} \sqrt{\frac{1}{3} l \cdot \ln(2k)} \right], \tag{11.7}$$

在以下定理 11.9 的证明中, 将说明这样的m, 可以在估计计算量时得到最优的上界.

令 $r_1 = 4P(m), r_2 = 2r_1/\varepsilon$, 其中 $\varepsilon = \binom{P(m)+u}{u}/p^m$, ε 是任取整数 b 使 g^b 为光滑元的概率的下界. 随机选取最多 r_2 个 b, 要求从诸 g^b 中找出 r_1 个光滑元. 设置 I 的初始值为零, 假设已经找到了光滑元 $\{R_i\}$ $(1 \leqslant i \leqslant I)$, 这时再任取 b, 计算 $g^b = cR$, 若 R 是光滑元, 但不能表为 $\{R_i\}$ $(1 \leqslant i \leqslant I)$ 的组合 (理解为向量), 则将 R 添加进 $\{R_i\}$, 并将 I 增加 1. 要求在选取 r_2 个 b 后, 能得到一个事实上的支架集, 将计算结果结束时的 I 记为 $I_{\max}$.

定理 11.8 当 $l \to \infty$ 时, 集合 $\{R_i\}$ $(1 \leqslant i \leqslant I_{\max})$ 不是事实上的支架集的概率趋于零.

证明 我们的算法失败, 可能有两种情况:

(1) 在 r_2 次尝试中没有可能找到 r_1 个光滑元.

(2) 从 r_1 个光滑元中产生的 $\{R_i\}$ $(1 \leqslant i \leqslant I_{\max})$ 不是事实上的支架集合.

现在分别估计这两个事件出现的概率的上界 P_1 和 P_2.

假定每次试验的成功概率为 δ, 在 N_2 次独立试验中, 成功的次数少于 N_1 的概率 P 适合

$$P \leqslant \frac{\delta(1-\delta)}{N_2(N_1/N_2)^2} \tag{11.8}$$

(这称为切比雪夫不等式).

考虑 P_1 的上界, 任取 b, 使 g^b 为光滑元的概率至少为 ε. 利用式 (11.8) 取 $\delta = \varepsilon$, $N_1 = r_1$, $N_2 = r_2$ 得到

$$P_1 \leqslant \frac{\varepsilon(1-\varepsilon)}{b_2(b_1/b_2)^2} < \frac{b_2 \varepsilon}{b_1^2} = \frac{1}{2P(m)}.$$

考虑 P_2 的上界, 把一个新向量添加进原有的 $\{R_i\}$ 理解为一次成功的试验, 所以每次试验成功概率是不同的, 它依赖于原有的 $\{R_i\}$, 但当 $\{R_i\}$ $(1 \leqslant i \leqslant I_{\max})$ 不是事实上的支架集时, 每次试验的成功概率至少为 1/2. 每个 R_i 是 $P(m)$ 维向量, 所以成功试验的次数一定少于$P(m)$, 取 $\delta = 1/2, N_1 = P(m), N_2 = r_1$, 由式 (11.8) 可得

$$P_2 \leqslant \frac{1}{P(m)}.$$

由式 (11.7) 及引理 11.4, 当 $l \to \infty$ 时, 可知 $P_1 + P_2 \to 0$, 证毕.

定理 11.9　*设 m 由式(11.7)给定, σ 为任一正数, 构造 $\{R_i\}$, $1 \leqslant i \leqslant I_{\max}$ 需要*

$$O\big(\exp\{(1+\sigma)\sqrt{12l \cdot \ln(2k)}\}\big)$$

次 F_{p^k} 中的运算, 其中 $l = k \cdot \ln p$.

证明　算法的第一步, 任取 r_2 个 b_i, 然后判断它是否是光滑元. g^{b_i} 的计算量为 $\ln b_i$ 阶, 这部分计算量可以忽略不记. 判断 g^{b_i} 是否是光滑元, 需用 S_m 中多项式逐个试除, 而由于 g^{b_i} 有重复因子, 增加的试除次数不超过 k, 所以总的试除次数不超过 $P(m)+k$, 算法第一步的计算量为 $O\big(r_2[P(m)+k]\big)$.

在算法的第二步, 每得到一个新的光滑元 $g^{b_i} = cR$, 都要用 Gauss 法检查 R 是否可以是已有 $\{R_i\}$ 的线性组合, R_i 的维数为 $P(m)$, 所以第二步的计算量为 $O\big(r_1[P(m)]^3\big)$. 因此构造 $\{R_i\}$, $1 \leqslant i \leqslant I_{\max}$ 的预运算总的计算量为

$$O\big(r_2[P(m)+k]\big) + O\big(r_1[P(m)]^3\big). \tag{11.9}$$

估计上式中两个量的上界, 由引理 11.4 及式 (11.7) 中 m 的选取可知 $P(m) \geqslant k$, 所以

$$O\big(r_2[P(m)+k]\big) = O\left(P(m)^2 p^k \frac{u!P(m)!}{(P(m)+u)!}\right),$$

利用 Stirling 公式, $n! \sim \sqrt{2n\pi}\left(\dfrac{n}{e}\right)^n$ $(n \to \infty)$, 上式右端可化为

$$O\left(P(m)^2 p^k \cdot \frac{u^u P(m)^{P(m)}}{(P(m)+u)^{P(m)+u}}\right) = O\left(P(m)^2 p^k \cdot \frac{u^u}{P(m)^u}\right).$$

再利用引理 11.4 及 $(k/m)-1 \leqslant u < k/m$, 上式右端化为

$$O\left(\frac{p^{2m+k}(k/m)^{k/m}}{(p^m/2m)^{(k/m)-1}}\right) = O\big(p^{3m}(2k)^{k/m}\big) = O\left(\exp\left\{3m\ln p + \frac{k}{m}\ln(2k)\right\}\right). \tag{11.10}$$

当 $m = \dfrac{1}{\ln p}\sqrt{(1/3)l \cdot \ln(2k)}$ 时, 上式达到最小值, 由于 m 为整数, 故取 m 为式 (11.7) 右端给定的值.

对任一 $\delta > 0$, 当 m 足够大时有

$$\frac{1}{(1+\delta)\ln p}\sqrt{(1/3)l \cdot \ln(2k)} \leqslant m \leqslant \frac{1}{\ln p}\sqrt{(1/3)l \cdot \ln(2k)},$$

将上式代入式 (11.10), 得到式 (11.9) 中第一项的上界

$$O\left(\exp\left\{\sqrt{3l \cdot \ln(2k)} + \frac{(1+\delta)k\ln p\ln(2k)}{\sqrt{(1/3)l \cdot \ln(2k)}}\right\}\right) = O\Big(\exp\big\{(1+\delta)\sqrt{12l \cdot \ln(2k)}\big\}\Big).$$

式 (11.9) 中第二项的上界可以类似地得到

$$O\big(b_1 P(m)^3\big) = O\big(P(m)^4\big) = O\big(p^{4m}\big) = O\Big(\exp\{4\sqrt{(1/3)l \cdot \ln(2k)}\}\Big),$$

定理证毕.

由定理 11.9 可见, 当 p 固定, $k \to \infty$ 时, F_{p^k} 上的指标计算法是一个亚指数算法, 从定理 11.9 的证明也可知道, 寻找光滑元的计算量大于求解线性方程组的计算量.

在基于离散对数的公钥密码方案设计中, 最常用的基群是 $\mathbb{Z}_p^*$. 以上已经介绍了 $\mathbb{Z}_p^*$ 的指标计算法, 然而数域筛法是目前求 $\mathbb{Z}_p^*$ 上离散对数的最快算法. 在用数域筛法分解大数的思想启发下, 1992 年, Gordon 首先设计了求 $\mathbb{Z}_p^*$ 上离散对数的数域筛法, 且估计算法的时间复杂度为 $L_p[1/3, 3^{1/2}]$[19]; 1993 年 Schirokauer 改进了 Gordon 的方法, 使期望时间复杂度达到 $L_p[1/3, (64/9)^{1/3}]$[46].

我们已经知道, 利用 11.2 节和 11.3 节的方法计算 $\mathbb{Z}_p^*$ 上离散对数的时间复杂度为 $O(\sqrt{q})$, 其中 q 是 $p-1$ 中的最大素因子. 为保障最大的安全强度, 实际应用中 q 一般取和 p 相当的素数, 即 $p-1 = rq$, r 是一个很小的数. 此时求 $\mathbb{Z}_p^*$ 上离散对数 $x = \log_u v$, 只需求 $x_1 \equiv x(\mathrm{mod}\ r)$ 和 $x_2 \equiv x(\mathrm{mod}\ q)$, 然后用中国剩余定理求得 $x = \log_u v$. 下面介绍用数域筛法求

$$x = \log_u v \,(\mathrm{mod}\ q).$$

数域筛法的目的是求得整数 s, t, 而且 $\gcd(t, q) = 1$, 使得 $u^s v^t$ 为 $\mathbb{Z}_p^*$ 中的 q 次幂, 即

$$u^s v^t = w^q,$$

那么,

$$x \equiv -st^{-1} \,(\mathrm{mod}\ q).$$

因此, 我们的思路是构造 $\mathbb{Z}_p^*$ 中的一个 q 次方幂, 使其能够写成 u 和 v 的次幂之乘积. 和大数分解的数域筛法一样, 首先构造一个环 $\mathbb{Z}[\alpha]$ 中的 q 次幂, 然后通过某个到 $\mathbb{Z}_p$ 的环同态, 得到 $\mathbb{Z}_p$ 中的一个 q 次幂. 具体地, 选择一个首一的整系数不可约多项式 $f(x)$ 和一个自然数 $m = 2^h v$, 使得 $f(m) \equiv 0(\mathrm{mod}\ p)$, 且 q 不整除 $d(f)$. 令 α 是 $f(x)$ 的一个根, 数域 $K = \mathbb{Q}(\alpha)$, 因为 q 在 K 不分歧, 故

$$qO_K = \wp_1 \cdots \wp_g,$$

令 $\varepsilon_i = N(\wp_i) - 1$, $\varepsilon = \mathrm{lcm}\,\{\varepsilon_i | i = 1, \cdots, g\}$, 那么对任意 $\omega \in O_K$, 有

$$\omega^\varepsilon \equiv 1 \,(\mathrm{mod}\ q),$$

这样可定义映射

$$\lambda:\Gamma=\{\omega\in O_K|q\nmid N(\omega)\}\longrightarrow\frac{qO_K}{q^2O_K}$$
$$\omega\longmapsto\omega^{\varepsilon}-1\,(\mathrm{mod}\ q^2O_K),$$

可验证 λ 是乘法半群 Γ 到加法群 $\dfrac{qO_K}{q^2O_K}$ 的同态.

引理 11.5　*令 U 是 O_K 的单位群, $U'=\{\eta\in U|\eta\equiv 1(\mathrm{mod}\ q^2O_K)\}$, 假设 $U'\subseteq U^q$, 且 K 的类数 h_K 不被 q 整除. 若 $\omega\in\Gamma$ 满足*

(1) $\mathrm{ord}_{\wp}(\omega)\equiv 0(\mathrm{mod}\ q)$, *对 O_K 中所有的素理想 $\wp$;*

(2) $\lambda(\omega)=0$,

则 ω 是 O_K 中 q 次方幂.

证明　由条件 (1) 可知, 存在理想 I 使得 $(\omega)=I^q$, 又由于 q 不整除 h_K, 故 I 也是主理想, 设为 (δ), 那么存在 $u\in U$, 使得 $\omega=\delta^q u$. 而 $\lambda(\omega)=0$ 意味着 $\omega^{\varepsilon}\equiv 0(\mathrm{mod}\ q^2)$, 故 $1\equiv\omega^{\varepsilon}=(\delta^{\varepsilon})^q u^{\varepsilon}\equiv u^{\varepsilon}(\mathrm{mod}\ q^2)$, 所以 $u\in U'\subseteq U^q$, 即 u 是一个 q 次方幂, ω 也是 O_K 中 q 次方幂.

注　假设 K 是随机选取的一个代数数域, 那么 K 满足引理 11.5 的条件的概率是很大的, 详情可见文献 [46]. 在以下讨论中, 不妨设 K 满足引理 11.5 的条件.

取 O_K 的一组整基 $\{\alpha_1,\cdots,\alpha_n\}$, $\omega^{\varepsilon}-1$ 能够写成 $q(a_1\alpha_1+\cdots+a_n\alpha_n)$, $a_i\in\mathbb{Z}$, 定义同态映射

$$\lambda_i:\quad\Gamma\longrightarrow\mathbb{Z}_q$$
$$\omega\longmapsto a_i\,(\mathrm{mod}\ q),$$

故 $\lambda(\omega)=0$ 当且仅当 $\lambda_i(\omega)=0$, $i=1,\cdots,n$.

筛法是构造集合 $S=\{(a,b)\big|\,|a|\leqslant s,\,1\leqslant b\leqslant t,\,\gcd(a,b)=1,\,(a+bm)N(a+b\alpha)\,B\text{-光滑}\}$, 使得 $|S|\geqslant|S_Q|+|S_K|+n-1$, 同大数分解数域筛法一样, 令 $g(x,y)=x+my$, $\overline{f}=y''f\left(-\dfrac{x}{y}\right)$, 用筛法能寻找满足这两个齐次多项式的光滑值.

下面描述数域筛法的大致步骤.

(1) 选取 m, $f(x)$ 同上, 定义环同态

$$\phi:\quad\mathbb{Z}[\alpha]\longrightarrow\mathbb{Z}_p$$
$$g(\alpha)\longmapsto g(m),$$

然后选择合适的一个界 B, 构造有理因子基 $FQ=\{p\text{素数}\,|\,p\leqslant B\}$, 代数因子基 $\mathrm{FK}=\{\wp\subseteq\mathbb{Z}[\alpha]|\wp\text{是一次素理想},\,N(\wp)\leqslant B\}$.

(2) 筛法是构造集合 $S=\{(a,b)\big|\,|a|\leqslant s,\,1\leqslant b\leqslant t,\,\gcd(a,b)=1,\,(a+bm)N(a+b\alpha)\,B\text{-光滑}\}$, 使得 $|S|\geqslant|S_Q|+|S_K|+n-1$, 同大数分解数域筛法一样, 令 $g(x,y)=$

$x+my$, $\overline{f}=y''f\left(-\dfrac{x}{y}\right)$, 用筛法能寻找满足这两个齐次多项式的光滑值.

对每个 $(a,b)\in S$,

$$\left|a+bm\right|=\prod_{p\in S_Q}p^{e_p(a,b)},\quad \left|a+b\alpha\right|=\prod_{\wp\in S_K}\wp^{e_\wp(a,b)}.$$

(3) 构造 $d=|S_Q|+|S_K|+n-1$ 维 $\mathbb{Z}_q$ 上的向量:

$$\nu(a,b)=\big(e_p(a,b)(\bmod q), e_\wp(a,b)(\bmod q), \lambda_j(a+b\alpha)(\bmod q)\big)_{p\in S_Q,\,\wp\in S_K,\,1\leqslant j\leqslant n},$$

$$\nu(u)=\big(e_p(u)(\bmod q), e_\wp=0, \lambda_j=0\big)_{p\in S_Q,\,\wp\in S_K,\,1\leqslant j\leqslant n},$$

$$\nu(v)=\big(e_2=h,\ e_p=0,\ e_\wp(\alpha)=0,\ \bmod q,\ \lambda_j(a)(\bmod q)\big)_{2\neq p\in S_Q,\,\wp\in S_K,\,1\leqslant j\leqslant n}.$$

从集合 $\{x(a,b)\,|\,(a,b)\in S\}$ 中选取 $(d-1)$ 个元素, 使其和 $\nu(u)$ 构成一组基

$$\big\{\nu(a,b)\,\big|\,(a,b)\in S'\subseteq S\big\}\cup\{\nu(u)\},$$

然后将这 d 个向量作为列向量构成可逆矩阵 A, 解 $\mathbb{Z}_q$ 上的线性方程组

$$AX=-\nu(v)',$$

求得解 $\big(x(a,b),x(u)\big)_{(a,b)\in S'}$. 那么由引理 11.5 可知

$$\alpha\prod_{(a,b)\in S'}(a+b\alpha)^{x(a,b)}$$

是 $\mathbb{Z}[\alpha]$ 中的 q 次方幂,

$$u^{x(u)}2^h\prod_{(a,b)\in S'}(a+bm)^{x(a,b)}\,(\bmod p)$$

是 $\mathbb{Z}_p$ 中的 q 次幂. 而

$$u^{x(u)}2^h\prod_{(a,b)\in S'}(a+bm)^{x(a,b)}\equiv u^{x(u)}v^{-1}m\prod_{(a,b)\in S'}(a+bm)^{x(a,b)}\,(\bmod p),$$

故

$$\log_u(v)\equiv x(u)\,(\bmod q).$$

Adelman[1] 将数域筛法类比到函数域中, 提出函数域筛法来求 $F_{p^m}^*$ 上的离散对数, 只要 p 不是很大, 函数域筛法的期望时间复杂度为 $L_{p^m}[1/3,c]$, $c>0$ 是一个常数, 且当 p 取 2 时, 该算法恰是 Coppersmith 算法[11].

第 12 章　超椭圆曲线

12.1　超椭圆曲线的 Jacobian

为了简化, 假设域 F 的特征 $\neq 2$(特征为 2 的情况见文献 [24]). 假设定义在 F 上的多项式

$$f(x) = x^{2g+1} + a_1 x^{2g} + \cdots + a_{2g+1}$$

没有重根. 方程

$$y^2 = f(x) \tag{12.1}$$

在仿射平面上定义一条曲线, 该曲线上各点都是非奇异的. 将方程 (12.1) 化为齐次方程

$$Y^2 Z^{2g-1} = X^{2g+1} + a_1 X^{2g} Z + \cdots + a_{2g+1} Z^{2g+1},$$

可见, 上述曲线在射影平面上完备化后, 增加唯一的点 $\mathcal{O} = (0, 1, 0)$, 称为无穷远点, 当 $g > 1$ 时, 它是一个奇异点. 称射影曲线

$$\mathcal{C} = \{(\alpha, \beta) \mid \alpha, \beta \in \overline{F},\ \beta^2 = f(\alpha)\} \cup \{(0, 1, 0)\}$$

为亏格 g 的超椭圆曲线. 当 $g = 1$ 时, 它就是椭圆曲线. $\mathcal{C}$ 上除 $\mathcal{O}$ 之外的点都称为有限点.

设点 $Q = (\alpha, \beta) \in \mathcal{C}$, 则 $\overline{Q} = (\alpha, -\beta) \in \mathcal{C}$ 称为 Q 的反点. 当 $\beta \neq 0$ 时, $Q \neq \overline{Q}$, 这时 $f(\alpha) \neq 0$, 取 $x - \alpha$ 为 Q 点的单值化子 ($x - \alpha$ 在 Q 点有一阶零点). 当 $\beta = 0$ 时, $Q = \overline{Q}$, 这时 $f(\alpha) = 0$, 取 y 为 Q 的单值化子, 易见 $\mathrm{ord}_Q(x - \alpha) = 2$.

设 $p(x, y) \in \overline{F}[x, y]$, 由于 $y^2 = f(x)$, 作为 $\mathcal{C}$ 上的函数 $p(x, y)$ 可表为 $\overline{p}(x, y) = a(x) - b(x)y$, 其中 $a(x), b(x) \in \overline{F}[x]$. 考虑 $p(x, y)$ 在 $\mathcal{C}$ 的点 Q 的阶.

(1) 若 $Q = (\alpha, \beta)$ 为有限点. 设 $\overline{p} = (x - \alpha)^{r_0}(a_0(x) - b_0(x)y)$, $(x - \alpha)$ 不能同时整除 $a_0(x)$ 和 $b_0(x)$. 若 $a_0(\alpha) - b_0(\alpha)\beta \neq 0$, 则

$$\mathrm{ord}_Q P = \begin{cases} r_0, & Q \neq \overline{Q}, \\ 2r_0, & Q = \overline{Q}. \end{cases}$$

若 $a_0(\alpha) - b_0(\alpha)\beta = 0$, 则

$$\mathrm{ord}_Q P = \begin{cases} r_0 + r, & Q \neq \overline{Q}, \\ 2r_0 + 1, & Q = \overline{Q}, \end{cases}$$

其中 $r>0$ 适合

$$a_0(x)-b_0(x)y=\sum_{i=r}^{\infty}d_i(x-\alpha)^i.$$

r 可利用

$$(x-\alpha)^r \parallel a_0(x)^2-b_0(x)^2f(x) \tag{12.2}$$

决定. 由于 $b_0(\alpha)\neq 0$(若 $b_0(\alpha)=0$, 则 $a_0(\alpha)=0$, 不可能), 故 $b_0(x)\neq 0$, 则有

$$\left(\frac{a_0(x)}{b_0(x)}-\frac{1}{b_0(x)}\sum_{i=r}^{\infty}d_i(x-\alpha)^i\right)^2-f(x)=0,$$

因而

$$a_0(x)^2-b_0(x)^2f(x)=2a_0(x)\sum_{i=r}^{\infty}d_i(x-\alpha)^i-\left(\sum_{i=r}^{\infty}d_i(x-\alpha)^i\right)^2,$$

若 $x-\alpha\nmid a_0(x)$, 可见式 (12.2) 成立; 若 $x-\alpha\mid a_0(x)$, 由于 $x-\alpha\nmid b_0(x)$, 可见, $(x-\alpha)^2\mid f(x)$, 但 $f(x)$ 没有重根, 这不可能.

当 $Q=\overline{Q}$ 时, $\beta=0$, 这时 $a_0(\alpha)=0$, $b_0(\alpha)\neq 0$. 因 y 是 Q 的单值化子, 可见, $\mathrm{ord}_Q(a_0(x)-b_0(x)y)=1$, 且 $x-\alpha\parallel a_0(x)^2-b_0(x)^2f(x)$(注意 $x-\alpha\parallel f(x)$).

(2) 若 $Q=\mathcal{O}$. 由于 $y^2=x^{2g+1}+x$的低次项, 可取 $\mathrm{ord}_{\mathcal{O}}(x)=-2$, $\mathrm{ord}_{\mathcal{O}}(y)=-2g-1$, 所以

$$\mathrm{ord}_{\mathcal{O}}p=-\max(2\deg a(x),2g+1+2\deg b(x)).$$

由 $\mathcal{C}$ 上的点 Q_i 组成的有限形式和 $D=\sum m_iQ_i$ $(m_i\in\mathbb{Z})$ 称为 $\mathcal{C}$ 的一个除子, 所有除子组成加法群 $\mathcal{D}$. 除子 D 的次数 $\deg D=\sum m_i$, 所有次数为零的除子组成 $\mathcal{D}$ 的一个子群 $\mathcal{D}^\circ$. 当 $p(x,y)$ 在 $\mathcal{C}$ 上不恒为零时, 定义函数 $p(x,y)\in\overline{F}[x,y]$ 对应的除子 $\mathrm{div}(p)=\sum\limits_{Q}\mathrm{ord}_Q(p)$, 由代数曲线的一般理论, 可知 $\mathrm{div}(p)\in\mathcal{D}^\circ$. 设 $p(x,y)/q(x,y)$ 为 $\mathcal{C}$ 上的有理函数, 当 p,q 不在 $\mathcal{C}$ 上恒为零时, 令 $\mathrm{div}(p/q)=\mathrm{div}(p)-\mathrm{div}(q)$. $\mathcal{C}$ 上任一有理函数对应的除子称为主除子, 由主除子生成 $\mathcal{D}^\circ$ 的子群记为 $\mathbb{P}$. 商群 $\mathcal{D}^\circ/\mathbb{P}$ 称为超椭圆曲线 $\mathcal{C}$ 上的 Jacobian. 除子 $D_1,D_2\in\mathcal{D}^\circ$, 当 $D_1-D_2\in\mathbb{P}$ 时, 记 $D_1\sim D_2$, 称 D_1 与 D_2 线性等价.

设 $Q=(\alpha,\beta)\in\mathcal{C}$, 当 $\beta\neq 0$ 时, 则有 $\mathrm{div}(x-\alpha)=Q+\overline{Q}-2\mathcal{O}$, 所以 $-Q\sim\overline{Q}-2\mathcal{O}$, 当 $\beta=0$ 时, 则有 $\mathrm{div}(x-\alpha)=2Q-2\mathcal{O}$, 所以 $2Q\sim 2\mathcal{O}$. 设 $D=\sum m_iQ_i$ 为 $\mathcal{D}^\circ$ 中任一除子, 利用上述性质, 可知 D 一定与一个形如 $\sum m_iQ_i-(\sum m_i)\mathcal{O}$ 的除子线性等价, 它具有下述性质: 每个系数 $m_i>0$, 当 Q_i 在和式中出现时, $\overline{Q}_i(\neq Q)$ 一定不在和式中出现, 当 $Q_i=\overline{Q}_i$ 时, Q_i 的系数为 1. 具有这种性质的除子称为半既约

的. 在一个半既约的除子中, 若 $\sum m_i \leqslant g$, 则称它为既约除子. 利用 Riemann-Roch 定理, 一定存在一个函数 f, 使 $D+(f) \geqslant -g\mathcal{O}$(因 $l(D+g\mathcal{O}) \geqslant g-g+1=1$), 所以 $\mathcal{D}^\circ$ 中任一除子一定与一个既约除子线性等价, 也可以证明这样的既约除子是唯一的[25].

超椭圆曲线的 Jacobian 是一个加法群. 我们给 Jacobian 中每个元素一个恰当的表达式, 并找出它的加法的运算法则.

设 $D=\sum m_i Q_i-(\sum m_i)\mathcal{O}$ 是 $\mathcal{D}^\circ$ 中一个半既约除子, $Q_i=(\alpha_i,\beta_i)$. 令 $a(x)=\prod(x-\alpha_i)^{m_i}$, $b(x)\in \overline{F}[x]$ 适合下述条件: $b(\alpha_i)=\beta_i(\forall i)$, $a(x) \mid\mid b(x)^2-f(x)$ (式 (12.2)), $\deg b(x)<\deg a(x)$, 这样的 $b(x)$ 是唯一确定的. 易见除子 D 线性等价与 $\gcd(\operatorname{div}(a(x)), \operatorname{div}(b(x)-y))$ (不考虑 $\mathcal{O}$ 的部分). 为了简单起见, 今后我们表 $D=\operatorname{div}(a,b)$. 例如, 若 $Q=(\alpha,\beta)$, 则 $Q-\mathcal{O}=\operatorname{div}(x-\alpha,\beta)$, $2Q-2\mathcal{O}=\operatorname{div}\big((x-\alpha)^2, (f'(\alpha)(x-\alpha)+2\beta^2)/2\beta\big)$. 当且仅当 $\deg a(x)\leqslant g$ 时, $\operatorname{div}(a,b)$ 为既约除子.

设 $\operatorname{div}(a,b)=\operatorname{div}(a_1,b_1)+\operatorname{div}(a_2,b_2)$, 如何计算 a,b? 设 $d=\gcd(a_1,a_2,b_1+b_2)$ (多项式的最大公因子), 存在 $s_1(x), s_2(x), s_3(x)\in\overline{F}[x]$, 使

$$s_1a_1+s_2a_2+s_3(b_1+b_2)=d,$$

则

$$\begin{aligned} &a=a_1a_2/d^2,\\ &b=(s_1a_1b_2+s_2a_2b_1+s_3(b_1b_2+f))/d \pmod a, \end{aligned} \tag{12.3}$$

可以直接验证上述计算公式是正确的[8], 该计算方法实际上是通过 (虚) 二次代数函数域 $\overline{F}(x,y)$ 中类群的加法得来的, 为了更好地理解这个算法, 将在 12.2 节讨论 $\overline{F}(x,y)$ 的类群的加法.

考虑两个特殊的情况:

(1) 当 a_1 与 a_2 互素时, 则 $d=1$, 可取 $s_3=0$, 这时

$$a=a_1a_2,\quad b=s_1a_1b_2+s_2a_2b_1(\bmod a).$$

(2) 当 $a_1=a_2$, $b_1=b_2$(即计算一个除子的 2 倍) 时, 可取 $s_2=0$.

上述计算得到的 $\operatorname{div}(a,b)$ 不一定是既约的, 一般地, 任一半既约的除子表达式可利用下述方法化为既约的表达式. 取

$$\begin{aligned} &a'=(f-b^2)/a,\\ &b'\equiv -b(\bmod a'),\quad \deg b'<\deg a'. \end{aligned} \tag{12.4}$$

我们将在 12.2 节证明 $\operatorname{div}(a',b')\sim\operatorname{div}(a,b)$. 设 $\deg a=m$, $\deg b=n<m$, 则 $\deg a'=\max(2g+1,2n)-m$. 若 $m>g+1$, 则 $\deg a'\leqslant 2(m-1)-m=m-2$; 若

$m = g+1$, 则 $\deg a' = 2g+1-(g+1) = g$. 当 $\operatorname{div}(a,b)$ 不是既约形式时, 可以重复利用上述方法, 得到一个与它线性等价的既约除子. 这实际上是 Gauss 计算二次型既约形式的方法. 关于计算既约形式的改进算法可见[8, 51].

12.2　虚二次代数函数域

方程 (12.1) 定义的超椭圆曲线 $\mathcal{C}$ 的函数域 $\overline{F}(\mathcal{C}) = \overline{F}(x,y)$ 是有理函数域 $\overline{F}(x)$ 的二次扩域. 容易验证, $\overline{F}(\mathcal{C})$ 中的任一代数整函数一定形如 $a+by$, 其中 $a,b \in \overline{F}[x]$. 以 R 表示 $\overline{F}(\mathcal{C})$ 中所有代数整函数组成的环. $\overline{F}[x]$ 中所有素理想形如 $(x-\alpha)$ $(\alpha \in \overline{F})$, 它们在 R 中都分解为两个素理想 $\mathfrak{P}_1$, $\mathfrak{P}_2$ 之积 ($\mathfrak{P}_1$ 与 $\mathfrak{P}_2$ 可以相同). 记 $\beta^2 = f(\alpha)$, 当 $f(\alpha) \neq 0$ 时, $(x-\alpha)$ 分解为 $\mathfrak{P}_1 = (x-\alpha, y-\beta)$ 和 $\mathfrak{P}_2 = (x-\alpha, y+\beta)$ 之积, 当 $f(\alpha) = 0$ 时, $(x-\alpha)$ 分解为 $(x-\alpha, y)^2$. 可见, $\mathcal{C}$ 上的有限点与 R 中的素理想一一对应. 进一步地, $\mathcal{D}^\circ$ 中的除子 (仅考虑有限点部分) 与 R 的分式理想一一对应, 且两个除子之和对应的理想为它们各自对应的理想之积, 主除子对应主理想, 所以 $\mathcal{C}$ 的 Jacobian 与 R 的类群同构. 当 $D = \sum m_i Q_i - (\sum m_i)\mathcal{O}$ 为半既约除子时, D 对应 R 的一个理想 $\prod (x-\alpha_i, y-\beta_i)^{m_i}$, 其中 $Q_i = (\alpha_i, \beta_i)$.

设 $\mathfrak{R}$ 为 R 的一个整理想. 令

$$M = \{m(x) \in \overline{F}[x] \mid m(x) \in \mathfrak{R}\},$$
$$N = \{n(x) \in \overline{F}[x] \mid \exists m \in \overline{F}[x], \text{使} m + ny \in \mathfrak{R}\},$$

M 和 N 都是 $\overline{F}[x]$ 中的主理想, 设 $M = (u)$, $N = (v)$, 则存在 $r + vy \in \mathfrak{R}$, 使

$$\mathfrak{R} = (u, r+vy).$$

由于 $uy \in \mathfrak{R}$, 故 $v|u$, 又 $y(r+vy) = vf + ry \in \mathfrak{R}$, 故 $v|r$. 记 $u = av$, $r = bv$, 于是

$$\mathfrak{R} = v(a, b+y) \sim (a, b+y),$$

($\sim$ 表示理想的等价), 可以认为 $\deg b < \deg a$. 易见 $(b+y)(b-y) = b^2 - f \in \mathfrak{R} \cap \overline{F}[x]$, 故 $a|b^2 - f$. 记 $b^2 - f = ac$, 由于 f 无重因子, 可见 $\gcd(a,b,c) = 1$(对比 12.1 节中除子的半既约形式).

设 $\mathfrak{R}_i = (a_i, b_i + y)$, $\deg b_i < \deg a_i$, $b_i^2 - f = a_i c_i$ $(i = 1,2)$. 设 $\mathfrak{R}_1\mathfrak{R}_2 \sim (a, b+y)$, $\deg b < \deg a$, $b^2 - f = ac$, 现计算 a 和 b. 记 $\gcd(a_1, a_2, b_1+b_2) = d$, 则存在 $s_1, s_2, s_3 \in \overline{F}[x]$, 使 $d = s_1 a_1 + s_2 a_2 + s_3(b_1+b_2)$. 记 $a_1 = a_1' d, a_2 = a_2' d, b_1 + b_2 = hd$, 从而 $s_1 a_1' + s_2 a_2' + s_3 h = 1$. 由于 $b_1 b_2 + f = b_1 b_2 + b_i^2 - a_i c_i = b_i(b_1+b_2) - a_i c_i$, 所以 $d \mid b_1 b_2 + f$, 则有

$$\mathfrak{R}_1\mathfrak{R}_2 = (a_1 a_2,\ a_1(b_2+y),\ a_2(b_1+y),\ b_1 b_2 + f + (b_1+b_2)y).$$

显然,

$$s_1a_1(b_2+y)+s_2a_2(b_1+y)+s_3(b_1b_2+f+(b_1+b_2)y)=d(b+y)\in\mathfrak{R}_1\mathfrak{R}_2,$$

其中

$$b=(s_1a_1b_2+s_2a_2b_1+s_3(b_1b_2+f))/d=s_1a_1'b_2+s_2a_2'b_1+s_3(b_1b_2+f)/d,$$

所以

$$\begin{aligned}\mathfrak{R}_1\mathfrak{R}_2&=\big(a_1a_2,\ a_1(b_2+y),\ a_2(b_1+y),\ b_1b_2+f+(b_1+b_2)y,\ d(b+y)\big)\\&=d\left(a_1'a_2'd,\ a_1'(b_2-b),\ a_2'(b_1-b),\ \frac{b_1b_2+f}{d}-hb,\ b+y\right).\end{aligned}$$

由于

$$\begin{aligned}b_2-b&=b_2(1-s_1a_1')-s_2a_2'b_1-s_3(b_1b_2+f)/d\\&=b_2(s_2a_2'+s_3h)-s_2a_2'b_1-s_3(b_2h-a_2'c_2)\\&=a_2'(b_2s_2-s_2b_1+s_3c_2),\end{aligned}$$

所以 $a_2'\mid b_2-b$, 同理 $a_1'\mid b_1-b$. 又

$$\begin{aligned}&\frac{b_1b_2+f}{d}-hb\\=&\frac{b_1b_2+f}{d}\Big(s_1a_1'+s_2a_2'+s_3h\Big)-h\Big(s_1a_1'b_2+s_2a_2'b_1+s_3\frac{b_1b_2+f}{d}\Big)\\=&-a_1'a_2'(s_1c_2+s_2c_1),\end{aligned}$$

现在来证明 $a_1'a_2'\in\mathfrak{R}_1\mathfrak{R}_2/d$. 由于 $da_1'a_2'\in\mathfrak{R}_1\mathfrak{R}_2/d$,

$$\begin{aligned}(b_1-b_2)a_1'a_2'&=a_1'a_2'(b_1-b)-a_1'a_2'(b_2-b)\in\mathfrak{R}_1\mathfrak{R}_2/d,\\c_1a_1'a_2'&=\frac{b_1+b_2}{d}a_2'(b_1+y)-a_2'\Big(\frac{b_1b_2+f}{d}+\frac{b_1+b_2}{d}y\Big)\in\mathfrak{R}_1\mathfrak{R}_2/d,\end{aligned}$$

故 $\gcd(d,\ c_1,\ b_1-b_2)\cdot a_1'a_2'\in\mathfrak{R}_1\mathfrak{R}_2/d$. 实际上, $\gcd(d,\ c_1,\ b_1-b_2)=1$, 否则, 若有不可约多项式 $p(x)\gcd(d,c_1,b_1-b_2)$, 则 $p\mid a_1,\ p\mid c_1$, 由 $p\mid b_1+b_2,\ p\mid b_1-b_2$ 可得 $p\mid b_1$, 但 $\gcd(a_1,b_1,c_1)=1$, 这不可能. 所以证明了 $a_1'a_2'\in\mathfrak{R}_1\mathfrak{R}_2/d$. 最后得到

$$\mathfrak{R}_1\mathfrak{R}_2\sim(a,b+y),$$

其中 $a=a_1'a_2'$. 可以设 $\deg b<\deg a$. 我们得到了 R 中两个理想类合成的算法, 也就是说 12.1 节中给出的 $\mathcal{C}$ 上的 Jacobian 中两个点相加的算法.

设 a',b' 为 12.1 节中式 (12.4) 所给, 由于

$$(a,b+y)\sim\big(a(b-y),\ b^2-y^2\big)\sim\big(c,-b+y\big)=\big(a',b'+y\big),$$

所以 $\mathrm{div}(a,b)=\mathrm{div}(a',b')$.

12.3 基于超椭圆曲线的公钥密码

设 $\mathcal{C}$ 为有限域 F_q 上由方程 $y^2 = f(x)$ 定义的超椭圆曲线. 类似基于椭圆曲线的公钥密码, 可以建立基于 $\mathcal{C}$ 的 Jacobian $J(F_q)$ 上的公钥密码 (实际上, 椭圆曲线即是亏格 $g = 1$ 的超椭圆曲线, 椭圆曲线的点生成的群是与它的 Jacobian 同构的).

选取一个除子 $D \in J(F_q)$, 要求 D 的阶是一个大素数. 每个用户选取私钥 k, 将 $D' = kD$ 作为该用户的公钥. 由于 $D' = \mathrm{div}(a', b')$, 多项式 a', b' 的系数即可作为公钥使用. 利用下述方法, 可以在 $J(F_q)$ 中随机选取一个基点 D. 设正整数 $m \leqslant g$, 随机选取 $\alpha \in F_{q^m}$, 当 $f(\alpha)$ 为 F_{q^m} 中的平方元 (此情况发生的概率为 50%) 时, 计算 $f(\alpha)$ 的平方根 β, 则 $Q = (\alpha, \beta) \in \mathcal{C}$. 这时

$$D = \sum_{\sigma \in Gal(F_{q^m}/F_q)} Q^\sigma - m\mathcal{O}$$

为 $J(F_q)$ 中的除子. 在计算 $D' = kD$ 时, 需要用到 12.1 节的算法.

已知 $D_1, D_2 \in J(F_q)$, 且 $D_1 \in \langle D_2 \rangle$, 计算 m, 使 $D_1 \sim mD_2$, 这就是超椭圆曲线上的离散对数问题 (HECDLP). 基于超椭圆曲线的公钥密码的安全性是建立在计算 HECDLP 的复杂度之上. 在第 11 章介绍的小步–大步法和袋鼠法等一般的计算 DLP 的方法, 显然也适用于 HECDLP. FR 约化和 SSSA 约化也可推广到 HECDLP[51]. 当亏格 g 与 F_q 的特征相比较大时, Adelman, de Marrais 和 Huang 猜想有一个计算 HECDLP 的亚指数算法, 这是一个很有趣的理论结果, 他们的方法利用了大整数因子分解的数域筛法的思想.

目前, 基于超椭圆曲线的公钥密码的应用还没有提上日程.

第 13 章　格

格的概念最早出现在 19 世纪数论和晶体学的研究中. 作为 m 维实空间 $\mathbb{R}^m$ 中的一个离散加法子群, 格往往具有无穷多组 $\mathbb{Z}$ 基, 而格的不同基表示会直接影响到一些具体问题求解的难易程度, 格基约化的目的就是针对某个具体研究问题, 寻找有利于该问题求解的格的好基表示, 其思想最早可追溯至 Lagrange 和 Gauss 等对二次型理论的研究. 1982 年, A.K. Lenstra, H.W. Lenstra 和 L. Lovăsz 给出了一种新的约化基, 且给出具体约化过程, 后被人们称为 LLL 算法. 基于格上的数学难题和相关求解算法的格理论在密码学中 (包括密码编码学和密码分析学) 得到了广泛的应用.

本章介绍格的基本理论及其在密码学中的应用, 首先简要介绍了格基本概念和 LLL 算法, 然后介绍了 LLL 算法在密码分析中的应用, 最后介绍了两类基于格中数学难题设计的公钥密码体制.

13.1　基 本 概 念

记 $\mathbb{R}$ 为实数集, $\mathbb{R}^m$ 为 m 维欧氏空间, $\mathbb{R}^m$ 的元素用列向量表示, $\mathbb{R}^m$ 中的内积为

$$\begin{aligned}\langle\cdot\rangle:\ \mathbb{R}^m\times\mathbb{R}^m &\longrightarrow \mathbb{R}\\ \langle u,v\rangle &\longmapsto u^{\mathrm{T}}v,\end{aligned}$$

u 与 v 的内积时常也简写为 uv, 此内积定义了 $\mathbb{R}^m$ 中向量的长度

$$\begin{aligned}\|\cdot\|:\ \mathbb{R}^m &\longrightarrow \mathbb{R}\geqslant 0\\ u &\longmapsto \|u\|=\langle u,u\rangle^{\frac{1}{2}}=(u^{\mathrm{T}}u)^{\frac{1}{2}},\end{aligned}$$

进一步地, 可定义 $\mathbb{R}^m$ 中任意两个向量 u 和 v 之间的距离为 $\|u-v\|$.

记 $\mathrm{B}_m(x,r)$ 为 $\mathbb{R}^m$ 中以 x 为球心, r 为半径的开球, 即

$$\mathrm{B}_m(x,r)=\{y\in\mathbb{R}^m|\|y-x\|<r\}.$$

在 m 确定的情况下, 可将 $\mathrm{B}_m(x,r)$ 简写为 $\mathrm{B}(x,r)$.

定义 13.1　$\mathbb{R}^m$ 的一个子集 D 称为离散的, 若满足对任意 $x\in D$, 都存在 $r>0$ 使得

$$\mathrm{B}(x,r)\cap D=\{x\}.$$

定义 13.2 $\mathbb{R}^m$ 的一个子集 L 称为格, 若 L 是离散的, 且构成 $\mathbb{R}^m$ 的一个加法子群.

显然, $\{0\}$ 和 $\mathbb{Z}^m$ 均是格, 分别称作零格和整格. 而 $\mathbb{Q}^m$ 和 $\mathbb{R}^m$ 都是 $\mathbb{R}^m$ 的加法子群, 但它们都不构成格.

例 13.1 取 $b_1, b_2 \in \mathbb{R}^2$ 是一组 $\mathbb{R}$ 线性无关向量, 记 $L(b_1, b_2)$ 为向量 b_1 和 b_2 所有的整系数线性组合构成的集合, 即 $L(b_1, b_2) = \mathbb{Z}b_1 + \mathbb{Z}b_2$, $L(b_1, b_2)$ 是一个格, 其几何表示见图 13.1, 是所有格点构成的集合.

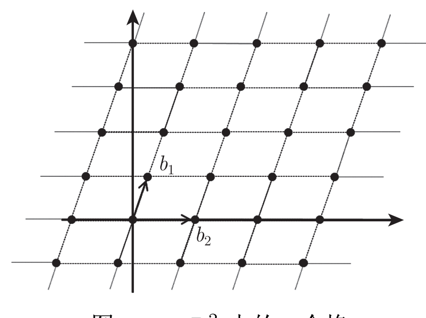


图 13.1 $\mathbb{R}^2$ 中的一个格

定理 13.1 令 L 是 $\mathbb{R}^m$ 的一个加法子群, 则

(1) L 是格当且仅当存在 $r > 0$ 使得 $\mathrm{B}(0, r) \cap L = \{0\}$;

(2) 格 L 的任意一个加法子群 L' 也构成格.

证明留作习题 (见习题 13.1). 此时的格 L' 称作格 L 的子格.

例 13.2 对任意给定的正整数 $a_1, \cdots, a_n \in \mathbb{N}$, 方程 $\sum\limits_{i=1}^{n} x_i a_i = 0$ 所有整数解构成一个格.

令 $A \subseteq \mathbb{R}^m$, 记 $\mathrm{span}(A)$ 为由 A 生成的 $\mathbb{R}$ 线性子空间.

定义 13.3 格 L 的维数 $\dim(L)$ 定义为向量空间 $\mathrm{span}(L)$ 的维数.

当 $\dim(L) = m$ 时, 称格 L 是满秩的.

设 $b_1, \cdots, b_n$ 是 $\mathbb{R}^m$ 中的 n 个向量, 记 $L(b_1, \cdots, b_n)$ 为向量组 $b_1, \cdots, b_n$ 所有整系数线性组合, 即

$$L(b_1, \cdots, b_n) = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n = \left\{ \sum_{i=1}^{n} n_i b_i \middle| \forall i, n_i \in \mathbb{Z} \right\}. \tag{13.1}$$

式 (13.1) 定义的集合 $L(b_1, \cdots, b_n)$ 是 $\mathbb{R}^m$ 的一个加法子群, 但未必构成格 (见习题 13.2). 下面的定理给出了集合 $L(b_1, \cdots, b_n)$ 构成格的充分条件.

定理 13.2 如果向量 $(b_1, \cdots, b_n)$ 满足下述条件之一, 则集合 $L(b_1, \cdots, b_n)$ 构成一个格:

(1) $b_1, \cdots, b_n \in \mathbb{Q}^m$;

(2) $b_1, \cdots, b_n \in \mathbb{R}^m$ 是 $\mathbb{R}$ 线性无关的.

证明　(1) 若 $b_1, \cdots, b_n \in \mathbb{Q}^m$, $L(b_1, \cdots, b_n)$ 构成格是显然的;

(2) 定义平行多面体 P 为

$$P = \left\{ \sum_{i=1}^{m} x_i b_i \middle| |x_i| < 1 \right\}.$$

由于 $b_1, \cdots, b_n$ 是 $\mathbb{R}$ 线性无关的, 所以有

$$L(b_1, \cdots, b_n) \cap P = \{0\}.$$

适当选取足够小的 $r > 0$, 使得 $\mathrm{B}(0, r) \subseteq P$ 是容易的. 由定理 13.1 可知结论成立, 证毕.

以后常用一组 $\mathbb{R}$ 线性无关组 $b_1, \cdots, b_n$ 按式 (13.1) 来构造一个格 $L(b_1, \cdots, b_n)$, 显然 $\dim(L(b_1, \cdots, b_n)) = n$, 称 $b_1, \cdots, b_n$ 是其一组格基. 为方便表述, 也可将这一线性无关组 $b_1, \cdots, b_n$ 简记为如下矩阵的形式

$$B = (b_1, \cdots, b_n) \in \mathbb{R}^{m \times n}.$$

同时可将式 (13.1) 简记为

$$L(B) = \{Bx | x \in \mathbb{Z}^n\}.$$

通常格 $L(B)$ 还会有其他的格基, 如在例 13.1 中, 除了 b_1, b_2 是它的一组基外, 向量组 $b_1 + 2b_2$ 和 $2b_1 + 3b_2$ 也是它的一组格基 (图 13-2).

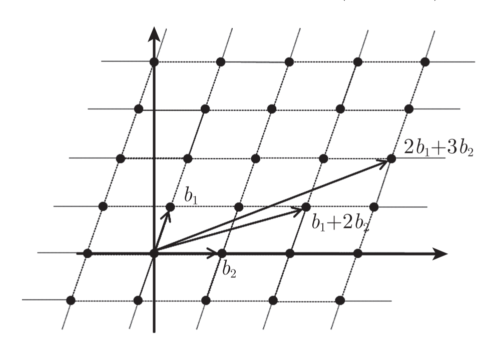


图 13.2　同一个格的两组基

若两组基 B 和 B' 生成了相同的格 (即 $L(B) = L(B')$), 则称 B 和 B' 是等价的, 关于格基的等价显然有如下结论.

定理 13.3　两组格基 $B, B' \in \mathbb{R}^{m \times n}$ 是等价的当且仅当存在一个幺模矩阵 $U \in \mathbb{Z}^{n \times n}$ (行列式为 1 或者 -1, 且所有项都为整数的方阵), 使得 $B' = BU$.

证明留作习题 (见习题 13.3).

取格 L 的一组格基 $(b_1,\cdots,b_n)$, 其对应的格拉姆 (Gram) 矩阵 $\triangle(b_1,\cdots,b_n)$ 定义为下面的 $n\times n$ 方阵

$$\triangle(b_1,\cdots,b_n)=(\langle b_i,b_j\rangle)=B^{\mathrm{T}}B.$$

容易看出矩阵 $\triangle(b_1,\cdots,b_n)$ 一定是正定的 (习题 13.4). 虽然同一个格的不同基所对应的格拉姆矩阵可能会不相同, 但由定理 13.3 可知, 不同基对应的格拉姆矩阵的行列式是相等的. 由此, 可以定义格 L 的判别式 $\det(L)$ 为任一格基对应的格拉姆矩阵行列式的平方根, 即

$$\det(L)=\sqrt{\det(B^{\mathrm{T}}B)}.$$

若格 L 是满秩的 (即 $n=m$), 且 $B=(b_1,\cdots,b_n)$ 是格 L 的一组基, 不难看出

$$\det(L)=|\det(B)|.$$

对于格 L 的一组基 $\{\alpha_1,\cdots,\alpha_n\}$, 定义

$$\Pi(\alpha_1,\cdots,\alpha_n)=\left\{\sum_{i=1}^{n}a_i\alpha_i\,\middle|\,0\leqslant a_i<1\right\}$$

是 $\mathbb{R}^n$ 中的一个平行多面体, 用 μ 表示 $\mathbb{R}^n$ 上的 Lebesgue 测度, 那么 $\Pi(\alpha_1,\cdots,\alpha_n)$ 的 "体积"$\mu(\Pi(\alpha_1,\cdots,\alpha_n))=\det(L)$(习题 13.6), 显然这和基的选取无关.

数论的一个分支 "数的几何" 中一个最重要的问题就是在一个给定区域里是否存在 (进而构造出) 某个事先给定的格中的非零向量. Minkowski 定理是这一方向的一个主要结论.

定理 13.4(Minkowski) 设 L 是 $\mathbb{R}^m$ 中的 n 维格, A 是 $\mathbb{R}^m$ 中一个可测的关于原点对称(即 $\alpha\in A\Rightarrow-\alpha\in A$)的凸集 $\left(\text{即 }\alpha,\beta\in A\Rightarrow\dfrac{1}{2}(\alpha+\beta)\in A\right)$, 若 $\mu(A)\geqslant 2^n\det(L)$, 则 $A\cap L$ 中有非零向量.

证明 参见文献 [53].

推论 13.1 对任意正整数 n, 一定存在一个常数 r_n, 满足对 $\mathbb{R}^n$ 中的任意一个满秩的格 L, 存在 L 中非零元素 x, 使得 $\|x\|^2\leqslant r_n\det(L)^{\frac{2}{n}}$. 最好可能的值 r_n 称作 Hermite 常数.

证明 构造一个闭区域 $A=\{(x_1,\cdots,x_n)\in\mathbb{R}^n|\ x_1^2+\cdots+x_n^2\leqslant c\}$, 其中 c 是一个待定的正实数. 令 $y_i=\dfrac{1}{\sqrt{c}}x_i$, $A=\{(y_1,\cdots,y_n)|\ y_1^2+\cdots+y_n^2\leqslant 1\}$, 那么 $\mu(A)=\displaystyle\int\cdots\int_A \mathrm{d}x_1\cdots\mathrm{d}x_n=c^{\frac{n}{2}}\cdot\delta_n$, 其中 $\delta_n=\displaystyle\int\cdots\int_A\mathrm{d}y_1\cdots\mathrm{d}y_n$. 为了利用 Minkowski 定理, 只需取 c 充分大, 满足

$$\mu(A)=c^{\frac{n}{2}}\cdot\delta_n=2^n\det(L),$$

即 $c = r_n \det(L)^{\frac{2}{n}}$, 其中 $r_n = 4\delta_n^{-\frac{2}{n}}$. 此时存在 $0 \neq x \in A \cap L$, 使

$$\|x\|^2 \leqslant r_n \det(L)^{\frac{2}{n}},$$

证毕.

对格问题进行研究时, 格中向量的长度问题常常值得关注. 格的 Minkowski 第 i 小量, 记为 $\lambda_i(L)(1 \leqslant i \leqslant n)$, 定义为包含至少 i 个线性无关格向量, 且以原点为球心的 “球体” 的最小半径. 它可以由下面的式子刻画

$$\lambda_i(L) = \inf\{r |\dim(\text{span}(L \cap \mathrm{B}_m(0, r))) \geqslant i\}. \tag{13.2}$$

在式 (13.2) 中, dim 表示维数, 而 inf 表示取下确界. 显然, Minkowski 第 1 小量就是格中最短非零向量的长度. 关于 Minkowski 第 1 小量有如下定理.

定理 13.5　对于 $\mathbb{R}^m$ 中任意的 n 维格 L, 都有

$$\lambda_1(L) \leqslant \sqrt{n} \cdot \sqrt[n]{\det(L)}.$$

证明　记集合 $\mathrm{S} = \mathrm{B}_m(0, \sqrt{n} \cdot \sqrt[n]{\det(L)} \cap \text{span}(L)$, 显然, S 是 span$(L)$ 中一个以原点为球心, 以 $\sqrt{n} \cdot \sqrt[n]{\det(L)}$ 为半径的 “球体”, 其 Lebesgue 测度大于 $\mu(\mathrm{S}) \geqslant 2^n \cdot \det(L)$, 则由定理 13.4 可知, 在 S 中存在格上非零向量 $v \in L \setminus \{0\}$, 此即 $\lambda_1(L) \leqslant \sqrt{n} \cdot \sqrt[n]{\det(L)}$. 证毕.

在格理论研究中, 最短向量问题和最近向量问题是最常用的, 它们定义如下.

定义 13.4(最短向量问题, 简记为 SVP)　给定格 L 的一组基 $B = (b_1, \cdots, b_n) \in \mathbb{R}^{m \times n}$, 求格$L$中的一个非零最短向量 Bx(即 $x \in \mathbb{Z}^n \setminus \{0\}$), 即满足对所有的 $y \in \mathbb{Z}^n \setminus \{0\}$, 都有

$$\|Bx\| \leqslant \|By\|.$$

定义 13.5(最近向量问题, 简记为 CVP)　给定格 L 的一组基 $B = (b_1, \cdots, b_n) \in \mathbb{R}^{m \times n}$ 和一个向量 $t \in \mathbb{R}^m$, 求格 L 中与向量 t 最近的向量 Bx, 即满足对所有的 $y \in \mathbb{Z}^n$, 都有

$$\|Bx - t\| \leqslant \|By - t\|.$$

最短向量问题和最近向量问题都是 NP-完全问题 (参见文献 [55], [56]). 与之相关的有以下判定性问题.

定义 13.6(判定性最短向量问题)　给定格 L 的一组基 $B = (b_1, \cdots, b_n) \in \mathbb{R}^{m \times n}$ 和数 $r > 0$, 判定格 L 中是否存在非零向量 Bx, 满足

$$\|Bx\| \leqslant r.$$

定义 13.7(判定性最近向量问题) 给定格 L 的一组基 $B=(b_1,\cdots,b_n)\in\mathbb{R}^{m\times n}$、一个向量 $t\in\mathbb{R}^m$ 和一个数 $r>0$, 判定格 L 中是否存在向量 Bx, 满足

$$\|Bx-t\|\leqslant r.$$

显然, 判定性最短向量问题和判定性最近向量问题的难度都不会高于对应的计算性问题, 但判定性最近向量问题仍是 NP-完全问题 (见文献 [63]1.2.2 节), 而判定性最短向量问题是 NP-难问题 (见文献 [63]4.3 节). 在研究上述问题的过程中, 下述两个问题相继被提出.

定义 13.8(近似最短向量问题, 简记为 SVP_λ) 给定正实数 λ 和一组格基 $B=(b_1,\cdots,b_n)\in\mathbb{R}^{m\times n}$, 求格 $L(B)$ 中的一个非零"较短"向量 Bx, 满足对所有 $y\in\mathbb{Z}^n\setminus\{0\}$, 都有

$$\|Bx\|\leqslant\lambda\cdot\|By\|.$$

定义 13.9(近似最近向量问题, 简记为 CVP_λ) 给定正实数 λ 和一组格基 $B=(b_1,\cdots,b_n)\in\mathbb{R}^{m\times n}$ 和一个向量 $t\in\mathbb{R}^m$, 求格 $L(B)$ 中与向量 t"较近"的向量 Bx, 满足: 对所有 $y\in\mathbb{Z}^n$, 都有

$$\|Bx-t\|\leqslant\lambda\cdot\|By-t\|.$$

当 $1<\lambda\leqslant n^{\frac{1}{\log\log n}}$ 时, SVP_λ 和 CVP_λ 都还是 NP-难问题, 见文献 [57], [58].

定义 13.10(最短无关向量问题, 简记为 SIVP) 给定一组格基 $B=(b_1,\cdots,b_n)\in\mathbb{R}^{m\times n}$, 求格 $L(B)$ 上 k $(k\leqslant n)$ 个长度不大于 $\lambda_k(L(B))$ 的线性无关的向量.

定义 13.11(近似最短无关向量问题, 简记为 SIVP_λ) 给定正实数 λ 和一组格基 $B=(b_1,\cdots,b_n)\in\mathbb{R}^{m\times n}$, 求格 $L(B)$ 上 k $(k\leqslant n)$ 个长度不大于 $\lambda\cdot\lambda_k(L(B))$ 的线性无关的向量.

SIVP 是 NP-完全问题 (见文献 [59]). 容易看出 SVP 是 SIVP 在 $k=1$ 时的特例.

13.2 LLL 算法

格 L 往往有许多 $\mathbb{Z}$ 基, 对处理某类问题时, 有些基会比其他基好些, 在应用中有时希望基是由一些长度较短的向量构成. 这类基称作约化基, 约化基的概念很早就有, 且还有最优约化基的概念, 如 Minkowski 约化基是格基按照长度和字典式构成的偏序下的最短基. 当维数为 1 和 2 时, 利用欧几里得算法或 Gauss 算法计算最优约化基是容易的. 但当维数大于等于 3 时, 至今也没有找到构造这类约化基的多项式时间算法 (也许并不存在). 因此从算法的角度, 往往需要在约化基和构造此约

化基的算法之间来个折中. 1982 年, A.K. Lenstra, H.W. Lenstra 和 L. Lovǎsz 给出了一种新的约化基, 且给出具体约化过程, 该算法也称为 LLL 算法. 当格的维数大于等于 3 时, LLL 算法虽然不能彻底解决 SVP 问题或 CVP 问题, 但可以解决近似因子为 $O\left(\left(\frac{2}{\sqrt{3}}\right)^n\right)$ 的 SVP 或 CVP 问题 (见文献 [71] 第 6 章).

在介绍 LLL 算法之前, 下面先给出对一组基的正交化过程. 对 $\mathbb{R}^m$ 中的任意一组线性无关向量 $b_1, \cdots, b_n$, 均可对其正交化, 得到一组正交向量 $b_1^*, \cdots, b_n^*$, 且这两组向量生成相同的线性空间.

引理 13.1(Schmidt 正交化) 令 $b_1, \cdots, b_n$ 是欧几里得空间 $\mathbb{R}^m$ 的一组线性无关向量, 归纳定义

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

其中 $\mu_{i,j} = b_i \cdot b_j^* / b_j^* \cdot b_j^* (1 \leqslant j < i \leqslant n)$, 那么 $\{b_i^*\}_{1 \leqslant i \leqslant n}$ 生成 $\mathbb{R}^m$ 的一组正交向量, 且

$$\sum_{j=1}^{i-1} \mathbb{R} b_j = \sum_{j=1}^{i-1} \mathbb{R} b_j^* \quad (2 \leqslant i \leqslant n).$$

特别地, 格 $L = \mathbb{Z} b_1 + \cdots + \mathbb{Z} b_n$ 的判别式

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\|, \quad \det(L) \leqslant \prod_{i=1}^{n} \|b_i\|.$$

该引理证明不复杂, 留作习题 (习题 13.5).

引理 13.2(Hadamard 不等式) 令 $A = (a_{ij})_{n \times n}$ 是 $\mathbb{R}$ 上一个 n 阶方阵, 那么

$$|\det A| \leqslant \prod_{1 \leqslant i \leqslant n} \left(\sum_{1 \leqslant j \leqslant n} |a_{ij}|^2 \right)^{\frac{1}{2}}.$$

证明 若 A 是奇异矩阵, 结论平凡. 设 A 是非奇异矩阵, b_i 是 A 的第 i 列构成的向量, 令 L 是由 $b_1, \cdots, b_n$ 生成的格, 由上述性质知

$$|\det A| = \det(L) \leqslant \prod_{1 \leqslant i \leqslant n} \|b_i\| = \prod_{1 \leqslant i \leqslant n} \left(\sum_{1 \leqslant j \leqslant n} |a_{ij}|^2 \right)^{\frac{1}{2}},$$

证毕.

定义 13.12 格 L 的一组基 $b_1, \cdots, b_n$ 称作 LLL 约化的, 如果满足

$$\begin{cases} \|\mu_{i,j}\| \leqslant \dfrac{1}{2}, & 1 \leqslant j < i \leqslant n, \\ \|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \geqslant \dfrac{3}{4} \|b_{i-1}^*\|^2, & 1 < i \leqslant n. \end{cases}$$

定理 13.6 若 $b_1, b_2, \cdots, b_n$ 是格 L 的一组 LLL 约化基, 那么

(1) $\det(L) \leqslant \prod_{i=1}^{n} \|b_i\| \leqslant 2^{\frac{n(n-1)}{4}} \det(L)$;

(2) $\|b_j\| \leqslant 2^{\frac{i-1}{2}} \|b_i^*\|, \quad 1 \leqslant j < i \leqslant n$;

(3) $\|b_1\| \leqslant 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}$;

(4) 对 L 中任一线性无关向量组 $x_1, \cdots, x_t$, 一定有

$$\|b_j\| \leqslant 2^{\frac{n-1}{2}} \max\{\|x_1\|, \cdots, \|x_t\|\} \qquad (1 \leqslant j \leqslant t).$$

特别地, 对 L 中任意非零元素 x, 有 $\|b_1\| \leqslant 2^{\frac{n-1}{2}} \|x\|$.

证明 因为 $b_1, \cdots, b_n$ 是 LLL 约化的, 显然条件

$$\left\|b_i^* + \mu_{i,i-1} b_{i-1}^*\right\|^2 \geqslant \frac{3}{4} \left\|b_{i-1}^*\right\|^2,$$

等价于

$$\left\|b_i^*\right\|^2 \geqslant \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \left\|b_{i-1}^*\right\|^2,$$

故 $\|b_i^*\|^2 \geqslant \dfrac{1}{2} \|b_{i-1}^*\|^2$, 于是直接可得

$$\|b_j^*\|^2 \leqslant 2^{i-j} \|b_i^*\|^2, \quad i \geqslant j. \tag{13.3}$$

因为 $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$, 所以

$$\begin{aligned} \|b_i\|^2 &= \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\|^2 \leqslant \|b_i^*\|^2 \left(1 + \frac{1}{4}\left(\sum_{j=1}^{i-1} 2^{i-j}\right)\right) \\ &= \frac{2^{i-1}+1}{2} \|b_i^*\|^2 \leqslant 2^{i-1} \|b_i^*\|^2, \end{aligned} \tag{13.4}$$

故

$$\det(L) \leqslant \prod_{i=1}^{n} \|b_i\| \leqslant \prod_{i=1}^{n} \left(2^{\frac{i-1}{2}} \|b_i^*\|\right) = \det(L) 2^{\sum_{i=1}^{n} \frac{i-1}{2}} = 2^{\frac{n(n-1)}{4}} \det(L).$$

(1) 得证.

由式 (13.3) 和式 (13.4) 知

$$\|b_j\| \leqslant 2^{\frac{j-1}{2}} \|b_j^*\| \leqslant 2^{\frac{j-1}{2} + \frac{i-j}{2}} \|b_i^*\| = 2^{\frac{i-1}{2}} \|b_i^*\|, \quad 1 \leqslant j \leqslant i \leqslant n.$$

(2) 得证.

令 (2) 中 $j=1$, i 取遍 1 到 n, 得

$$\|b_1\|^n \leqslant 2^{\frac{1}{2}\sum\limits_{i=1}^{n} i-1} \prod_{i=1}^{n} \|b_i^*\| = 2^{\frac{n(n-1)}{4}} \det(L),$$

即

$$\|b_1\| \leqslant 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}.$$

(3) 得证.

设 $x_i = \sum\limits_{j=1}^{n} a_{i,j} b_j$, $a_{i,j} \in \mathbb{Z}$, $1 \leqslant i \leqslant t$. 因为 $x_1, \cdots, x_t$ 线性无关, 所以一定存在 i, $1 \leqslant i \leqslant t$, $j_0 \geqslant t$, 使得 $a_{i,j_0} \neq 0$ 且 $a_{i,j} = 0$, $j > j_0$, 此时, $x_i = \sum\limits_{j=1}^{j_0} a_{i,j} b_j$, 且 x_i 在 $b_1^*, \cdots b_n^*$ 表示下, 有

$$x_i = \sum_{j=1}^{j_0} r_{i,j} b_j^*, \quad r_{i,j} \in \mathbb{R}.$$

由 b_j^* 和 b_j 的关系, 显然 $r_{i,j_0} = a_{i,j_0}$, 故

$$\begin{aligned} \|x_i\|^2 &= \sum_{j=1}^{j_0} r_{i,j}^2 \|b_j^*\|^2 \geqslant r_{i,j_0}^2 \|b_{j_0}^*\|^2 \\ &= a_{i,j_0}^2 \|b_{j_0}^*\|^2 \geqslant \|b_{j_0}^*\|^2 \\ &\geqslant 2^{1-j_0} \|b_j\|^2, \quad 1 \leqslant j \leqslant t \leqslant j_0 \qquad (\text{由}(2)), \end{aligned}$$

即 $\|b_j\| \leqslant 2^{\frac{j_0-1}{2}} \|x_i\| \leqslant 2^{\frac{n-1}{2}} \|x_i\| \leqslant 2^{\frac{n-1}{2}} \max\{\|x_1\|, \cdots \|x_t\|\}$, 证毕.

推论 13.2　若 $b_1, b_2, \cdots, b_n$ 是格 L 的一组 LLL 约化基, 且 $\min\limits_{1 \leqslant i \leqslant n} \|b_i^*\| \geqslant 1$, 则 $\|b_2\| \leqslant 2^{\frac{n}{2}} \det(L)^{\frac{1}{n-1}}$.

证明　根据定理 13.6 可知

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\| \geqslant \|b_1^*\| \cdot \|b_2^*\|^{n-1} 2^{-\frac{(n-1)(n-2)}{4}} \geqslant \|b_2^*\|^{n-1} 2^{-\frac{(n-1)(n-2)}{4}}.$$

因此,

$$\|b_2^*\| \leqslant 2^{\frac{n-2}{4}} \det(L)^{\frac{1}{n-1}}.$$

而

$$\|b_2\|^2 \leqslant \|b_2^*\|^2 + \frac{1}{4}\|b_1\|^2 \leqslant 2^{\frac{n-2}{2}} \det(L)^{\frac{2}{n-1}} + 2^{\frac{n-5}{2}} \det(L)^{\frac{2}{n}} \leqslant 2^{\frac{n-1}{2}} \det(L)^{\frac{2}{n-1}},$$

故,

$$\|b_2\| \leqslant 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n-1}},$$

证毕.

在给出格基约化算法之前, 解释一下该算法的思想, 假设 $b_1, \cdots, b_{k-1}$ 已知是 LLL 约化了, 初始 $k=2$, 首先需要约化 b_k 使得 $|\mu_{k,j}| \leqslant \dfrac{1}{2}$ 对所有的 $j<k$, 只需适当选择 a_j, 用 $b_k - \sum\limits_{j<k} a_j b_j$ $(a_j \in \mathbb{Z})$ 取代 b_k 就能达到目的. 具体地, 假设 $|\mu_{k,j}| \leqslant \dfrac{1}{2}$, $l<j<k$, 取 $q=[0.5+\mu_{k,l}]$ 是最接近 $\mu_{k,l}$ 的整数, 若用 $b_k - qb_l$ 取代 b_k, 设变化后的参数 $\mu_{k,i}$ 为 $\lambda_{k,i}$, 显然,

$$\lambda_{k,i} = \begin{cases} \mu_{k,i}, & l<i<k, \\ \mu_{k,l}-q, & i=l, \end{cases}$$

故 $|\lambda_{k,i}| \leqslant \dfrac{1}{2}$, $(l-1)<i<k$, 重复上述过程即可达到目的.

令 $B_j = \|b_j^*\|^2$, 其次要约化 $b_1, \cdots, b_n$ 满足 Lovăsz 条件, 即

$$B_k \geqslant \left(\frac{3}{4} - \mu_{k,k-1}^2\right) B_{k-1}.$$

k 从取 2 开始, 若 Lovăsz 条件满足, k 增加 1, 否则交换 b_{k-1} 和 b_k, 且 k 减 1, 因为此时只知道 $b_1, \cdots, b_{k-2}$ 是 LLL 约化的.

交换 b_{k-1} 和 b_k 后, 必须观察 $B_i, \mu_{i,j}$ 的变化情况, 设交换后的基为 $a_1, \cdots, a_n$, 即 $a_{k-1}=b_k$, $a_k=b_{k-1}$, $a_i=b_i (i \neq k-1, k)$, 用 $C_i, \lambda_{i,j}$ 表示对应 $b_1, \cdots, b_n$ 的 $B_i, \mu_{i,j}$, 显然, $\lambda_{i,j}=\mu_{i,j}$, $1 \leqslant j<i \leqslant k-2$, $\lambda_{k-1,j}=\mu_{k,j}$, $\lambda_{k,j}=\mu_{k-1,j}$, $1 \leqslant j \leqslant k-2$. 因为

$$a_{k-1}^* = a_{k-1} - \sum_{j=1}^{k-2} \lambda_{k-1,j} a_j^* = b_k - \sum_{j=1}^{k-2} \mu_{k,j} b_j^* = b_k^* + \mu_{k,k-1} b_{k-1}^*, \tag{13.5}$$

$$C_{k-1} = \|a_{k-1}^*\| = \|b_k^*\|^2 + \mu_{k,k-1}^2 \|b_{k-1}^*\| = B_k + \mu_{k,k-1}^2 B_{k-1},$$

故

$$\lambda_{k,k-1} = \frac{a_k \cdot a_{k-1}^*}{C_{k-1}} = \frac{b_{k-1} \cdot a_{k-1}^*}{C_{k-1}} = \frac{\mu_{k,k-1} b_{k-1} b_{k-1}^*}{C_{k-1}} = \frac{\mu_{k,k-1} B_{k-1}}{C_{k-1}}, \tag{13.6}$$

即 $\lambda_{k,k-1} C_{k-1} = \mu_{k,k-1} B_{k-1}$ 是个不变量. 又因为

$$\begin{aligned} a_k^* &= a_k - \sum_{j=1}^{k-1} \lambda_{k,j} a_j^* = b_{k-1} - \lambda_{k,k-1} a_{k-1}^* - \sum_{j=1}^{k-2} \mu_{k-1,j} b_j^* \\ &= b_{k-1}^* - \lambda_{k,k-1} a_{k-1}^* = b_{k-1}^* - \lambda_{k,k-1} b_k^* - \lambda_{k,k-1} \mu_{k,k-1} b_{k-1}^* \quad (\text{由式 } (13.5)) \\ &= -\lambda_{k,k-1} b_k^* + \left(1 - \frac{\mu_{k,k-1}^2 B_{k-1}}{C_{k-1}}\right) b_{k-1}^* \quad (\text{由式 } (13.6)) \\ &= -\lambda_{k,k-1} b_k^* + \frac{B_k}{C_{k-1}} b_{k-1}^*, \end{aligned}$$

故

$$C_k = \|a_k^*\| = \lambda_{k,k-1}^2 B_k + \frac{B_k^2 B_{k-1}}{C_{k-1}^2} = d\frac{(\lambda_{k,k-1}C_{k-1})^2 B_k + B_k^2 B_{k-1}}{C_{k-1}^2}$$

$$= \frac{\mu_{k,k-1}^2 B_{k-1}^2 B_k + B_k^2 B_{k-1}}{C_{k-1}^2} = \frac{B_k B_{k-1}}{C_{k-1}},$$

即 $C_k C_{k-1} = B_k B_{k-1}$ 又是一个不变量. 当 $i > k$ 时,

$$\lambda_{i,k-1} = \frac{b_i a_{k-1}^*}{C_{k-1}} = \frac{b_i b_k^* + \mu_{k,k-1} b_i b_{k-1}^*}{C_{k-1}}$$

$$= \frac{C_k b_i b_k^* + C_k \mu_{k,k-1} \boldsymbol{b}_i b_{k-1}^*}{B_k B_{k-1}} = \frac{C_k}{B_{k-1}}\mu_{i,k} + \frac{C_k \mu_{k,k-1}}{B_k}\mu_{i,k-1},$$

而

$$\frac{C_k}{B_{k-1}} = \frac{B_k}{C_{k-1}} = \frac{C_{k-1} - \mu_{k,k-1}^2 B_{k-1}}{C_{k-1}} = 1 - \mu_{k,k-1}\lambda_{k,k-1},$$

$$\frac{C_k \mu_{k,k-1}}{B_k} = d\frac{B_{k-1}\mu_{k,k-1}}{C_{k-1}} = \lambda_{k,k-1},$$

因此

$$\lambda_{i,k-1} = \lambda_{k,k-1}\mu_{i,k-1} + (1 - \mu_{k,k-1}\lambda_{k,k-1})\mu_{i,k},$$

$$\lambda_{i,k} = \frac{b_i a_k^*}{C_k} = \frac{-\lambda_{k,k-1} b_k^* b_i + \dfrac{B_k}{C_{k-1}} b_{k-1}^* b_i}{C_k}$$

$$= \frac{-\lambda_{k,k-1} C_{k-1} b_i b_k^* + B_k b_i b_{k-1}^*}{B_k B_{k-1}}$$

$$= -\mu_{k,k-1}\mu_{i,k} + \mu_{i,k-1},$$

即

$$\begin{pmatrix} \lambda_{i,k-1} \\ \lambda_{i,k} \end{pmatrix} = \begin{pmatrix} \lambda_{k,k-1} & 1 - \mu_{k,k-1}\lambda_{k,k-1} \\ 1 & -\mu_{k,k-1} \end{pmatrix} \begin{pmatrix} \mu_{i,k-1} \\ \mu_{i,k} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \lambda_{k,k-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu_{k,k-1} \end{pmatrix} \begin{pmatrix} \mu_{i,k-1} \\ \mu_{i,k} \end{pmatrix}, \quad i = k+1, \cdots, n.$$

这样便可以给出如下 LLL 约化算法.

LLL 算法

输入: 格 L 的一组基 $b_1, \cdots, b_n$

输出: 格 L 的一组 LLL 约化基

1. (初始)$b_1^* \leftarrow b_1$, $B_1 \leftarrow \|b_1^*\|^2$
2. (正交化)For i from 2 to n do

   2.1 $b_i^* \leftarrow b_i$

2.2 For j from 1 to $(i-1)$ do

$$\mu_{i,j}=\frac{b_ib_j^*}{B_j},\qquad b_i^*\leftarrow b_i^*-\mu_{i,j}b_j^*$$

2.3 $B_i\leftarrow|b_i^*|$

3. (初始)$k\leftarrow 2$
4. 执行 $(\star)$ for $l=k-1$
5. if $B_k<\left(\dfrac{3}{4}-\mu_{k,k-1}^2\right)B_{k-1}$ then goto (6)

   执行 F$(\star)$ for $l=k-2,k-3,\cdots,1$

   if $k=n$ then 终止

   $k\leftarrow k+1$

   goto (4)
6. $\mu\leftarrow\mu_{k,k-1}$, $B\leftarrow B_k+\mu^2B_{k-1}$, $\mu_{k,k-1}\leftarrow\mu B_k/B$

   $B_k\leftarrow B_{k-1}B_k/B$, $B_{k-1}\leftarrow B$

   $\begin{pmatrix}b_{k-1}\\ b_k\end{pmatrix}\leftarrow\begin{pmatrix}b_k\\ b_{k-1}\end{pmatrix}$, $\begin{pmatrix}\mu_{k-1,j}\\ \mu_{k,j}\end{pmatrix}\leftarrow\begin{pmatrix}\mu_{k,j}\\ \mu_{k-1,j}\end{pmatrix}$, for $j=1,\cdots,k-2$

   $\begin{pmatrix}\mu_{i,k-1}\\ \mu_{i,k}\end{pmatrix}\leftarrow\begin{pmatrix}1&\mu_{k,k-1}\\ 0&1\end{pmatrix}\begin{pmatrix}0&1\\ 1&-\mu\end{pmatrix}\begin{pmatrix}\mu_{i,k-1}\\ \mu_{i,k}\end{pmatrix}$, for $i=k+1,\cdots,n$

   if $k>2$ then $k\leftarrow k-1$, goto (4)

   $(\star)$ if $|\mu_{k,l}|>\dfrac{1}{2}$ then

   $r\leftarrow\lfloor\mu_{k,l}+0.5\rfloor$; $b_k\leftarrow b_k-rb_l$

   $\mu_{k,j}\leftarrow\mu_{k,j}-r\mu_{l,j}$ for $j=1,2,\cdots,l-1$

   $\mu_{k,l}\leftarrow\mu_{k,l}-r$

由算法前的分析可知, 对算法的正确性只需证明 k 通过有限步之后一定达到 n 或 $k\leftarrow k-1$ 的步骤只有有限步, 即交换 b_{k-1} 和 $\boldsymbol{b}_k$ 的过程只有有限步. 设

$$d_i=\prod_{1\leqslant j\leqslant i}B_j=\det(b_rb_s)_{1\leqslant r,s\leqslant i},\quad 1\leqslant i\leqslant n,\quad D=\prod_{i=1}^{n-1}d_i>0.$$

显然在整个算法中, 只有在 b_{k-1} 和 b_k 交换之后, 即执行算法的第 6 步后才会变 D, 由于除 B_k 和 B_{k-1} 外, 其余的 B_i 不会发生变化, 而 B_kB_{k-1} 是不变量. 因此除

d_{k-1} 外, 其余的 d_i 是不会变的. B_{k-1} 的变化值

$$C_{k-1} = B_k + \mu_{k,k-1}^2 B_{k-1} < \frac{3}{4} B_{k-1},$$

故每次执行第 6 步, D 至少减小 $\frac{3}{4}$ 倍.

令 L_i 是由 $b_1, \cdots, b_i$ 构成的格, $S_i = \min\{\|\nu\|^2 | \ \nu \in L_i\}$. 由推论 13.1 可知

$$d_i \geqslant S_i^i r_i^{-i} \geqslant S_n^i r_i^{-i} \quad .$$

记 $r = \max\{r_i| \ 1 \leqslant i \leqslant n\}$ 是一个常数, $d_i \geqslant S_n^i r^{-i} = (S_n/r)^i$, $D = \prod\limits_{i=1}^{n-1} d_i \geqslant (S_n/r)^{\frac{n(n-1)}{2}}$, 即 D 有一个和 L 有关的正常数作为下界, 故执行第 6 步只有可能是有限次. 实际上, 该算法的时间复杂度为输入向量的分量的最大值、格的秩, 以及空间维度的多项式.

13.3 LLL 算法在密码分析中的应用

格基约化理论在密码学中的首次应用出现在 1983 年 Adleman 对 Merkle-Helllman 背包体制的分析. 此后的三十多年时间里, 格基约化算法被用来对多种不同类型密码算法 (包括背包加密、RSA 加密和 DSA 签名等密码算法) 进行分析. 本节以背包问题求解和 RSA 密码算法分析为例, 简要介绍格基约化理论在密码算法分析中的应用.

13.3.1 背包问题求解

1978 年, Merkel 和 Hellman 基于背包问题提出了一种公钥密码体制, 称为 MH 体制, MH 体制的一个显著特点就是加解密速度快, 遗憾的是, 这类密码体制所基于的背包问题在通常情况下都可以转化为格中的最短向量 (或者最近向量) 问题, 进而用格基约化算法进行求解, 因此这类密码体制在现实中是不安全的.

关于背包问题, 前面 8.4 节已有介绍. 简单来说, 背包问题就是在给定一些正整数 $a_1, \cdots, a_n \in \mathbb{N}$ 和 $s = \sum\limits_{i=1}^{n} x_i a_i, x_i \in \{0, 1\}$ 的前提下, 求所有的 x_i. 将此背包问题记为 $P(a_1, \cdots, a_n, s)$.

显然, 对给定的背包问题 $P(a_1, \cdots, a_n, s)$, 求下述线性方程

$$\sum_{i=1}^{n} x_i a_i = s$$

的整数解是容易的, 不妨设 $(y_1, \cdots, y_n)$ 是上述方程的一个解.

考虑如下齐次线性方程

$$\sum_{i=1}^{n} z_i a_i = 0, \tag{13.7}$$

设 A_i 为 a_i 和 a_n 的最小公倍数 (记为 $A_i = \mathrm{lcm}(a_i, a_n))(1 \leqslant i \leqslant n-1)$, 取

$$B = (b_1, b_2, \cdots, b_{n-1}) = \begin{pmatrix} \dfrac{A_1}{a_1} & 0 & \cdots & 0 \\ 0 & \dfrac{A_2}{a_2} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \dfrac{A_{n-1}}{a_{n-1}} \\ -\dfrac{A_1}{a_n} & -\dfrac{A_2}{a_n} & \cdots & -\dfrac{A_{n-1}}{a_n} \end{pmatrix}.$$

容易验证向量组 $(b_1, \cdots, b_{n-1})$ 构成 $L_{a_1,\cdots,a_n}$ 的一组基. 若 $(s_1, \cdots, s_n)$ 是背包问题 $P(a_1, \cdots, a_n, s)$ 的一个解, 则有

$$(y_1 - s_1, \cdots, y_n - s_n) \in L_{a_1,\cdots,a_n}.$$

向量 $(y_1 - s_1, \cdots, y_n - s_n)$ 与格中向量$\left(y_1 - \dfrac{1}{2}, \cdots, y_n - \dfrac{1}{2}\right)$ 距离为 $\dfrac{\sqrt{n}}{2}$, "非常接近". 上述分析表明, 背包问题可以转化为格中最近向量问题进行求解.

对于给定的背包问题 $P(a_1, \cdots, a_n, s)$, 定义其背包密度为

$$d = \frac{n}{\max\limits_{1 \leqslant i \leqslant n} \{\log_2 a_i\}}.$$

当 $d > 1$ 时, 背包问题 $P(a_1, \cdots, a_n, s)$ 存在多个不同的解 (习题 13.7), 因此为了避免出现解密结果不唯一, 所有背包体制所基于的背包问题都满足 $d \leqslant 1$ 的条件. 利用 LLL 等格基约化算法可以求格 $L_{a_1,\cdots,a_n}$ 的约化基, 可以证明: 当 $d < 0.9408$ 时, 可以以一定的概率求出格向量 $(y_1 - s_1, \cdots, y_n - s_n)$, 进而得到背包问题 $P(a_1, \cdots, a_n, s)$ 的解 $(s_1, \cdots, s_n)$(详细见文献 [68] 的定理 3.1).

13.3.2　针对 RSA 密码算法的小解密指数攻击

RSA 是目前使用最广泛的公钥密码体制, 关于它的安全性分析一直是密码学界研究的热点和重点, 总的来看, RSA 密码算法还是相对安全的. 但是在一些特定条件下, 比如用户的解密指数 d 比较 "小" 的时候, 可以利用格基约化算法对 RSA 密码算法进行分析.

事实上, 对于任意给定用户的 RSA 公钥 (e, N) 和私钥 d 都满足

$$ed \equiv 1 \pmod{\phi(N)},$$

所以存在 $k \in \mathbb{Z}$ 满足

$$ed + k\phi(N) = 1.$$

而 $\phi(N) = N - q - p + 1$, 记 $A = N + 1$, $s = -(p+q)$, 则有

$$k(A+s) \equiv 1 \pmod{e}.$$

若记 $e = N^{\alpha}$, 并假设 $\dfrac{\sqrt{N}}{2} < p, q < 2\sqrt{N}$, $d < N^{\delta}$, 则有

$$|k| < \frac{ed}{\phi(N)} \leqslant \frac{2ed}{N} < 2e^{1+\frac{\delta-1}{\alpha}}|s| < 3\sqrt{N} = 3e^{\frac{1}{2\alpha}}.$$

在不明显影响结论的前提下, 为叙述方便, 可忽略上式中的常数因子, 不妨设

$$|k| < e^{1+\frac{\delta-1}{\alpha}}|s| < e^{\frac{1}{2\alpha}}.$$

再记 $f(x,y) = x(A+y)-1$, $X = e^{1+\frac{\delta-1}{\alpha}}$, $Y = e^{\frac{1}{2\alpha}}$, 则至少存在一个整数对 (x_0, y_0)(如 $(x_0, y_0) = (k, s)$) 满足

$$f(x_0, y_0) = x_0(A + y_0) - 1 \equiv 0 \pmod{e}, \quad |x_0| < X \text{且} |y_0| < Y.$$

以多项式 $f(x,y)$ 为基础构造如下两类多项式 (正整数 m 为待优化参数)

$$g_{i,k}(x,y) = x^i f^k(x,y) e^{m-k},$$

$$h_{j,k}(x,y) = y^j f^k(x,y) e^{m-k}.$$

显然, 对任意的 $0 \leqslant k \leqslant m$ 都有

$$g_{i,k}(k,s) \equiv 0 \pmod{e^m}$$
$$h_{j,k}(k,s) \equiv 0 \pmod{e^m}.$$

为方便起见, 有时多项式和多项式向量之间不加区分, 由多项式 $g_{i,k}(x,y)$ 和 $h_{j,k}(x,y)$ 的构造可知, 它们都是 $\mathbb{R}$ 线性无关的. 由定理 13.2 知, 由 $g_{i,k}(Xx, Yy)$ 和 $h_{j,k}(Xx, Yy)$ 的系数向量可生成格. 用 LLL 等格基约化算法求该格的约化基. 只要约化基中前两个向量 (不妨记为 $f_1(x,y)$ 和 $f_2(x,y)$) 足够短, 满足下述定理.

定理 13.7　*设 $f(x,y) \in \mathbb{Z}[x,y]$ 是至多含有 w 项的二元多项式, N 是一个大整数. X 和 Y 均为正数, 若*

(1) 存在 $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, 满足

$$f(x_0, y_0) \equiv 0 \pmod{N}, \quad |x_0| < X \text{ 且 } |y_0| < Y,$$

(2) $\|f(Xx, Yy)\| < \dfrac{N}{\sqrt{w}}$,

则 $f(x_0, y_0) = 0$.

证明　事实上, 因为 $\|f(Xx,Yy)\| < \dfrac{N}{\sqrt{w}}$, 所以有

$$\begin{aligned}|f(x_0,y_0)| &= \left|\sum_{i,j} a_{i,j}x_0^i y_0^j\right| \\ &= \left|\sum_{i,j} a_{i,j}X^iY^j\left(\frac{x_0}{X}\right)^i\left(\frac{y_0}{Y}\right)^j\right| \\ &\leqslant \sum_{i,j}\left|a_{i,j}X^iY^j\left(\frac{x_0}{X}\right)^i\left(\frac{y_0}{Y}\right)^j\right| \\ &< \sum_{i,j}|a_{i,j}X^iY^j| \\ &\leqslant \sqrt{w}\|f(Xx,Yy)\| \\ &< N.\end{aligned}$$

又因为 $f(x_0,y_0)\equiv 0 \pmod N$, 所以有

$$f(x_0,y_0)=0.$$

此时根据定理 13.7 可知

$$f_1(k,s)=f_2(k,s)=0,$$

证毕.

因此通过求 f_1 和 f_2 的结式 $r(y)=\mathrm{Res}_x(f_1(x,y),f_2(x,y))$ 的小根, 即可求出 $y_0=s$, 进而可以分解 RSA 模数 N.

如何选取参数才能确保所得格的约化基的前两个向量可以满足定理 13.7 中的条件? 事实上, 对于某个取定的正整数 m, 取以下这些多项式

$$g_{i,k}(x,y)=x^if^k(x,y)e^{m-k},\quad \text{其中}k=0,\cdots,m,\quad i=0,\cdots,m-k;$$

$$h_{j,k}(x,y)=y^jf^k(x,y)e^{m-k},\quad \text{其中}k=0,\cdots,m,\quad j=0,\cdots,t.$$

t 为一待优化的参数, 以多项式 $g_{i,k}(Xx,Yy)$ 和 $h_{j,k}(Xx,Yy)$ 的系数可生成格 $L(m,t)$, 该格的维数和判别式计算如下

$$d=\dim(L(m,t))=\frac{m(m+1)}{2}+t(m+1), \tag{13.8}$$

$$\det(L(m,t))=e^{\frac{(m+1)(m+1)(2m+3t)}{6}}X^{\frac{(m+1)(m+1)(2m+3t)}{6}}Y^{\frac{(m+1)(m^2+(2+3t)m+3t^2+3t)}{6}}.$$

将 $X = e^{1+\frac{\delta-1}{\alpha}}$ 和 $Y = e^{\frac{1}{2\alpha}}$ 代入可得

$$\det(L(m,t)) = e^{\frac{8\alpha+4\delta-3}{12\alpha}m^3+o(m^3)+\frac{4\alpha+2\delta-1}{4\alpha}tm^2+o(tm^2)+\frac{1}{4\alpha}mt^2+o(mt^2)}. \tag{13.9}$$

由推论 13.2 的结论可知, 当

$$2^{\frac{d-1}{4}}\det(L(m,t))^{\frac{1}{d-1}} < \frac{e^m}{\sqrt{d}} \tag{13.10}$$

时, 格 $L(m,t)$ 的 LLL 约化基 $(B_1, B_2, \cdots, B_d)$ 中前两个向量 B_1 和 B_2 必然满足

$$\|B_1(Xx, Yy)\| \leqslant \|B_2(Xx, Yy)\| < \frac{e^m}{\sqrt{d}}.$$

此时 (k, s) 是多项式 $B_1(x, y)$ 和 $B_2(x, y)$ 公共的小根 (而非模 e^m 意义下), 即

$$B_1(k, s) = B_2(k, s) = 0.$$

联合式 (13.8) 和式 (13.9), 可知当

$$t = \frac{m(1-2\delta)}{2} \quad 且 \quad \delta < \frac{7-2\sqrt{6\alpha+1}}{6}$$

时, 式 (13.10) 即可满足. 一般情况下, 假定 $\alpha \approx 1$, 通过选取合适的 m 和 t, 则在 $\delta < \dfrac{7-2\sqrt{6\alpha+1}}{6} \approx 0.2847$ 时, 即有

$$B_1(k, s) = B_2(k, s) = 0.$$

然后, 通过求 $B_1(x, y)$ 和 $B_2(x, y)$ 公共的小根即可得到

$$s = -(p+q).$$

再由 $N = pq$ 即可求解 p 和 q, 即将用户的 RSA 模数 N 进行分解.

本节给出了对于使用 “小” 解密指数 RSA 的分析算法, 其主要思想是根据 RSA 密码算法的公私钥方程, 将用户私钥恢复问题转化为格中最短向量问题进行求解, 分析过程表明当 $d < N^{0.284}$ 时, 本节的分析算法有效.

13.4　基于格的密码体制设计

基于格中数学难题构造陷门函数, 从而设计公钥密码体制的工作最早出现在 1996 年, 在随后近 20 年的时间里, 陆续出现了很多基于格理论的公钥密码算法. 总的来看, 由于格具有一些特殊的代数结构属性, 基于它的密码体制往往具有以下几个明显特点:

(1) 目前大多数基于格的密码体制都可证明是安全的;

(2) 体制的安全性可归约为格中数学难题的最坏情形;

(3) 后量子时代的候选密码之一: 到目前为止, 相比 "传统" 计算, 还没有具有明显优势的量子算法可以用来求解格中的经典数学难题;

(4) 格的线性代数结构简单, 与 RSA 和 ECC 等传统密码算法涉及的模指运算相比, 格元素的运算 (即向量加) 快;

(5) 基于格的密码体制具有更丰富的功能, 除了实现最基本的加密功能, 一些密码体制还具有数据访问控制和密文域计算等功能.

本节以 NTRU 体制和基于格的一个全同态加密体制为例, 简要介绍基于格中数学难题进行密码体制的设计思路.

13.4.1　NTRU 体制

NTRU(Number Theory Research Unit) 体制是由美国布朗大学三位数学教授于 1996 年提出的公钥加密体制. 该体制密钥生成简单, 加密、解密的速度比 RSA 等著名算法快得多, 已经成为 IEEE P1363, PKC 等众多密码算法标准中的候选算法之一. 该体制包含系统参数生成以及密钥生成、加密、解密三个多项式时间算法.

参数生成　令 (N, p, q) 为三个正整数, 满足 $q > p$ 及 $\gcd(p, q) = 1$(通常 p 非常小), 环 $R = \mathbb{Z}[X]/(X^N - 1)$, R 中的元素以多项式的形式表示. 令 L_1 为 R中系数取自集合 $\{-1, 0, 1\}$ 的多项式集合, L_2 是 R 中系数取自 $\left[-\dfrac{p-1}{2}, \dfrac{p+1}{2}\right]$ 区间的多项式集合.

密钥生成算法　选取 $f, g \in L_1$, f 在模 p 和模 q 下均有逆元, 分别记为 f_p 和 f_q. 计算 $h \equiv f_q \cdot g \pmod q$, 公钥 $pk = h$, 私钥 $sk = f_p$.

加密算法　对于 $m \in L_2$, 随机选取 $\phi \in L_1$, 计算并输出密文

$$c \equiv (p\phi \cdot h + m) (\bmod\ q).$$

解密算法　令 $a \equiv f \cdot c \pmod q$, 输出明文 $m' \equiv f_p \cdot a \pmod p$.

NTRU加密体制的正确性很容易验证. 根据 NTRU 参数, 密钥和加解密过程可知

$$\begin{aligned} a &\equiv f \cdot c \pmod q \\ &= (f \cdot (p\phi \cdot h) + f \cdot m) \pmod q \\ &= (f \cdot (p\phi \cdot f_q \cdot g) + f \cdot m) \pmod q \\ &= (p\phi \cdot g) + f \cdot m \pmod q. \end{aligned}$$

由于 p 很小, $((p\phi \cdot g) + f \cdot m)$ 会以很大的概率满足各项系数都在 $\left[-\dfrac{q}{2}, \dfrac{q}{2}\right]$ 区间, 所以该式(mod q) 不会改变, 即 $a = p\phi \cdot g + f \cdot m$, 于是

$$a\,(\mathrm{mod}\ p) = f \cdot m\,(\mathrm{mod}\ p)$$

$$f_p \cdot a\,(\mathrm{mod}\ p) = f_p \cdot f \cdot m\,(\mathrm{mod}\ p) = m\,(\mathrm{mod}\ p).$$

截止到目前, 还无法从理论上给出 NTRU 体制安全的严格证明.Coppersmith 和 Shamir 提出将 NTRU 的私钥和一个 $2N$ 维的格相关联, 若格中的最短向量可解, 则 NTRU 体制是不安全的. 对公钥 $h = \sum_{i=1}^{N-1} h_i x^i$, 给定常数 k, 取一组 $2N$ 维向量

$$(b_1, b_2, \cdots, b_N, b_{N+1}, b_{N+2}, \cdots, b_{2N})$$

$$= \begin{pmatrix} k & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & k & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & k & 0 & 0 & \cdots & 0 \\ h_0 & h_{N-1} & \cdots & h_1 & q & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & h_2 & 0 & q & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ h_{N-1} & h_{N-2} & \cdots & h_0 & 0 & 0 & \cdots & q \end{pmatrix}.$$

将该组向量生成的格记为 L, 则 L 也可以表示为

$$L = \{(ku, v) \mid u \cdot h = v\,(\mathrm{mod}\ q),\ u, v \in \mathbb{R}\},$$

其中 u 和 v 的系数对应的向量分别为 u 和 v. 由于生成用户私钥的 (f, g) 满足 $f \cdot h = g\,(\mathrm{mod}\ q)$, 所以 L 中包含 (kf, g), 可以以一定的概率通过格中的最短向量来逼近私钥 (见文献 [70]).

研究者利用格理论还提出了一些类似的攻击方法, 这些攻击最终都需要有效的格归约算法来求出格中的最短向量, 但对于较高维数的格, 求解最短向量是困难的. 从目前研究来看, NTRU 算法与 RSA 算法和 ECC 算法的安全性比较如下表. 表中数值为体制安全参数的比特数, 处于同一行的不同类型体制的安全强度相当.

RSA	ECC	NTRU
512	113	167
1024	160	263
2048	282	503

13.4.2 基于 LWE 问题的全同态加密体制

全同态加密的思想由 Rivest 等在 1978 年首次提出的, 该思想源自 RSA 算法具有的乘法同态特性: 使用同一密钥的若干密文进行乘法运算, 对运算结果解密,

得到的明文等于这些密文对应明文的乘积. 若存在一个加密体制, 对各种运算都保持上述同态性质, 那么就可以实现在不解密的条件下对加密数据执行各种运算. 目前, 全同态加密应用前景广泛. 例如, 在数据库中的应用: 用户将隐私数据储存在一个不可信服务器中, 服务器无法解密这些数据, 但能够对用户的数据查询请求等类似操作进行处理, 并给出加密状态下的结果. 类似的应用还有很多, 特别是当前云计算环境下, 全同态加密为解决云计算网络中数据的安全性和可计算性的矛盾提供了一种切实可行的方案. 2009 年, Gentry 基于理想格提出第一个严格意义的全同态加密算法, 支持任意次数的密文加法/乘法运算. 随后, 学术界基于格上数学难题先后设计出一系列全同态加密算法, 本节介绍一个由 Brakerski 提出的基于格上容错学习 (learning with errors, LWE) 问题的算法.

在介绍加密算法之前, 先简要介绍一下与 LWE 问题相关的概念和结论.

定义 13.13(容错学习问题, 简记为 LWE)　对于正整数 n, $q=q(n)\geqslant 2$, $\mathbb{Z}_q$ 上的分布 χ, $s\in\mathbb{Z}_q^n$. 记 $A_{s,\chi}$ 为 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上由 $(a,a^{\mathrm{T}}\cdot s+e)$ 组成的分布, 其中 a 是 $\mathbb{Z}_q^n$ 上均匀分布的变量, e 取自分布 χ. LWE 问题是指给定 $(a,b)\in A_{s,\chi}$, 求 s 的问题.

判定性 LWE 问题 (记为 DLWE) 是指有效区分 $A_{s,\chi}$ 和 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上均匀分布的问题. 2009 年, Peikert[72] 证明, 对 $\mathbb{Z}_q$ 上离散 Gauss 分布 χ, DLWE 问题可归约为格上的 SIVP 问题.

在讨论全同态加密算法之前, 先介绍一个基于 LWE 的公钥加密体制, 该体制不是同态体制. 令 n 为格的秩, $q\geqslant 2$ 为正整数, $N=n\log q$, χ 是 $\mathbb{Z}_q$ 上的 Gauss 分布. 体制由密钥生成算法、加密算法、解密算法组成, 具体描述如下.

参数生成　随机选取 $t\leftarrow\chi^n$, 随机选取矩阵 $B\leftarrow\mathbb{Z}_q^{N\times n}$ 和一个向量 $e\leftarrow\chi^N$, 计算 $b:=Bt+2e$, 令 A 是一个 $n+1$ 列的矩阵, 第一列是 b, 后而 n 列是 $-B$. 令私钥 $sk=s\leftarrow(1,t[1],\cdots,t[n])\in\mathbb{Z}_q^{n+1}$, 公钥 $pk=A$.

加密算法　对明文 $m\in\mathbb{Z}_2$, 令 $m=(m,0,\cdots,0)\in\mathbb{Z}_q^{n+1}$, 随机选取 $r\leftarrow\mathbb{Z}_2^N$, 输出密文 $c=m+A^{\mathrm{T}}r\in\mathbb{Z}_q^{n+1}$.

解密算法　计算 $m=[[\langle c,s\rangle]_q]_2$, 输出 m.

容易验证该体制正确性:

$$[[\langle c,s\rangle]_q]_2=[[(m^{\mathrm{T}}+r^{\mathrm{T}}A)\cdot s]_q]_2=[[m+2r^{\mathrm{T}}e]_q]_2=m.$$

全同态公钥加密和普通公钥加密算法相比, 除密钥生成算法、加密算法和解密算法外, 还需要专门的同态运算算法来完成密文上的同态运算功能. 为实现对同态运算的支持, Brakerski 等提出了密钥转换技术和模数转换技术. 在介绍这两项技术之前, 首先介绍与它们相关的两个函数:

BitDecomp$(x \in \mathbb{Z}_q^n, q)$: 将 x 分解为比特表示形式, 即若 $x = \sum_{j=0}^{[\log q]} 2^j \cdot u_j$, 其中 $u_j \in \mathbb{Z}_2^n$, 则输出 $(u_0, u_1, \cdots, u_{[\log q]}) \in \mathbb{Z}_2^{n \cdot [\log q]}$;

Powersof 2$(x \in \mathbb{Z}_q^n, q)$: 对输入的 $x \in \mathbb{Z}_q^n$ 和模数 q, 输出 $(x, 2 \cdot x, \cdots, 2^{[\log q]} \cdot x) \in \mathbb{Z}_q^{n \cdot [\log q]}$.

引理 13.3　对于等长的向量 c, s, 有

$$\langle \text{BitDecomp}(c, q), \text{Powersof2}(s, q) \rangle = \langle c, s \rangle (\text{mod } q).$$

证明

$$\begin{aligned}\langle \text{BitDecomp}(c, q), \text{Powersof2}(s, q) \rangle &= \sum_{j=0}^{[\log q]} \langle u_j, 2^j \cdot s \rangle \\ &= \sum_{j=0}^{[\log q]} \langle 2^j \cdot u_j, s \rangle \\ &= \langle c, s \rangle \quad (\text{mod } q),\end{aligned}$$

证毕.

密钥转换　密钥转换技术包含以下两个算法:

SwitchKeyGen(s_1, s_2, n_1, n_2, q): 输入两个私钥向量、它们的维数以及体制的模数, 输出一个辅助信息 $\tau_{s_1 \to s_2}$.

SwitchKey$(\tau_{s_1 \to s_2}, c_1, n_1, n_2, q)$: 输入辅助信息 $\tau_{s_1 \to s_2}$, 使用 s_1 加密的密文, 输出为使用密钥 s_2 加密相同明文生成的新密文.

算法描述如下: SwitchKeyGen$(s_1 \in \mathbb{R}_q^{n_1}, s_2 \in \mathbb{R}_q^{n_2})$:

(1) 将 s_2 表示为 $(s_2[0], t)$ 的形式 (其中 $s_2[0] = 1$), 随机选取矩阵 $B' \leftarrow \mathbb{Z}_q^{N \times n_2}$ 和向量 $e \leftarrow \chi^N$, 计算 $b := B't + 2e$, 令 $A = (b, -B')$ 是一个 $n_2 + 1$ 列的矩阵.

(2) 把 Powersof2$(s_1) \in \mathbb{Z}_q^N$ 加到 A 的第一列, 得到一个矩阵 B.

(3) 输出 $\tau_{s_1 \to s_2} = B$.

SwitchKey$(\tau_{s_1 \to s_2}, c_1)$:

(1) 计算 $c_2 = \text{BitDecomp}(c_1)^{\mathrm{T}} \cdot B \in \mathbb{R}_q^{n_2}$,

(2) 输出 c_2.

引理 13.4　令 $s_1, s_2, q, A, B = \tau_{s_1 \to s_2}$ 为 SwitchKeyGen(s_1, s_2, n_1, n_2, q) 的输出, 令 $A \cdot s_2 = 2e_2$, 令 $c_1 \in \mathbb{Z}_q^{n_1}, c_2 \leftarrow \text{SwitchKey}(\tau_{s_1 \to s_2}, c_1)$, 那么有

$$\langle c_2, s_2 \rangle = 2 \langle \text{BitDecomp}(c_1), e_2 \rangle + \langle c_1, s_1 \rangle (\text{mod } q).$$

证明　$\langle c_2, s_2\rangle = \mathrm{BitDecomp}(c_1)^{\mathrm{T}} \cdot B \cdot s_2$

$$= \mathrm{BitDecomp}(c_1)^{\mathrm{T}} \cdot (2e_2 + \mathrm{Powersof2}(s_1))$$

$$= 2\langle \mathrm{BitDecomp}(c_1), e_2\rangle + \langle \mathrm{BitDecomp}(c_1), \mathrm{Powersof2}(s_1)\rangle$$

$$= 2\langle \mathrm{BitDecomp}(c_1), e_2\rangle + \langle c_1, s_1\rangle \ (\mathrm{mod}\ q),$$

证毕.

模数转换　对于整向量 x 及整数 $q > p > r$, 定义函数如下:

$\mathrm{Scale}(x, q, p, r)$: 输入向量 x 及整数 $q > p > r$, 输出 x' 是满足$x' = x\,(\mathrm{mod}\ r)$ 且与 $\left(\dfrac{p}{q}\right) \cdot x$ 距离最近的整向量.

定理 13.8　令 $q > p > r$ 为满足 $q = p = 1\,(\mathrm{mod}\ r)$ 的正整数, 令 $c \in \mathbb{Z}^n$, $c' \leftarrow \mathrm{Scale}(c, q, p, r)$, 那么对于任意满足 $\langle c, s\rangle_q < \dfrac{q}{2} - \dfrac{q}{p} \cdot \sum\limits_i s[i]$ 的 $s \in \mathbb{Z}^n$, 都有

$$[\langle c', s\rangle]_p = [\langle c, s\rangle]_q\,(\mathrm{mod}\ r).$$

证明　必存在 $k \in \mathbb{Z}$ 使

$$[\langle c, s\rangle]_q = \langle c, s\rangle - kq,$$

那么对同样的 k, 令

$$e_p = \langle c', s\rangle - kp.$$

注意到 $e_p = [\langle c', s\rangle]_p\,(\mathrm{mod}\ p)$, 由于 $\|e_p\| < p/2$, 故 $e_p = [\langle c', s\rangle]_p$, 于是在模 r 意义下, 有 $[\langle c', s\rangle]_p = e_p = \langle c', s\rangle - kp = \langle c, s\rangle - kq = [\langle c, s\rangle]_q$. 证毕.

由定理 13.8 可以看出, 任何一个不知道私钥, 仅知道其长度上界的计算者, 都可以将一个模数为 q、使用密钥 s、对应明文为 m 的密文 c(也就是 $m = [[\langle c, s\rangle]_q]_r$) 转化为一个模数为 p、使用相同密钥 s、对应明文为 m 的密文 c' (也就是 $m = [[\langle c', s\rangle]_p]_r$).

利用密钥转换和模数转换技术, 可以在前文所述公钥加密算法的基础上给出如下全同态加密算法. 设同态运算的电路级数 L, μ 为正整数, 选取一组参数 $\mathrm{params}_j = (q_j, n_j, N, \chi_j)$, 其中 $j \in [0, L]$, 模数 q_j 将会从 $q_L((L+1) \cdot \mu$ 比特) 逐步降到 $q_0(\mu$ 比特). 全同态体制的具体描述如下.

密钥生成算法　对于所有的 $j \in [0, L]$ (从 $j = L$ 开始, 到 $j = 0$ 结束), 做如下运算:

(1) 随机选取 $t \leftarrow \chi^n$, 令 $s_j \leftarrow (1, t[1], \cdots, t[n]) \in \mathbb{Z}_q^{n+1}$; 随机选取矩阵 $B \leftarrow \mathbb{Z}_q^{N\times n}$ 和一个向量 $e \leftarrow \chi^N$, 计算 $b := Bt + 2e$, 令 A_j 是一个 $n+1$ 列的矩阵, 第一列是 b, 后而 n 列是 $-B$.

(2) 计算 $s'_j \leftarrow s_j \otimes s_j$.

(3) 计算 $\tau_{s'_{j+1}\to s_j} \leftarrow \mathrm{SwitchKeyGen}(s'_{j+1}, s_j)$ (若 $j = L$ 则省略这一步).

私钥为 $sk = \{s_j | j \in [0, L]\}$, 公钥为 $pk = \{A_j | j \in [0, L]\} \cup \{\tau_{s'_{j+1}\to s_j} | j \in [0, L-1]\}$.

加密算法 对明文 $m \in \mathbb{Z}_2$, 令 $m = (m, 0, \cdots, 0) \in \mathbb{Z}_{q_L}^{n+1}$, 随机选取 $r \leftarrow \mathbb{Z}_2^N$, 输出密文 $c = m + {A_L}^{\mathrm{T}} r$.

解密算法 计算 $m = [[\langle c, s\rangle]_q]_2$, 输出 m. 设密文为 $\boldsymbol{c}$, 当前级数为 j, 计算 $m = [[\langle c, s_j\rangle]_{q_j}]_2$, 输出 m.

该体制中密文运算可分解为 FHE.Add, FHE.Mult 及 FHE.Refresh 三种运算, 分别代表同态加法, 同态乘法和密文更新运算.

同态加 输入使用同样的 s_j 进行加密的密文 c_1 和 c_2, 计算 $c_3 \leftarrow c_1 + c_2 \pmod{q_j}$, 输出 c_3.

同态乘 输入使用同样的 s_j 进行加密的密文 c_1 和 c_2, 计算 $c_3 \leftarrow c_1 \otimes c_2$, 输出 c_3.

加密算法的正确性很容易验证 (与本节开始介绍的公钥加密体制基本相同). 对同态计算而言, FHE.Add 的正确性很容易验证. c_1 和 c_2 同态乘法运算后的结果为 $c_3 = c_1 \otimes c_2$, 设当前模数为 q_j, 密钥为 s_j, 对 c_3 进行解密有

$$[[\langle c_3, s_j \otimes s_j\rangle]_{q_j}]_2 = [[e_1 \cdot e_2]_{q_j}]_2 = [e_1 \cdot e_2]_2 = [e_1]_2 \cdot [e_2]_2 = m_1 \cdot m_2.$$

但是, 同态乘法会后密文 c_3 将为 $(n+1)^2$ 维向量, 密文中噪声也将增长, 为此设计了 FHE.Refresh 运算, 应用密钥转换技术和模数转换技术做进一步处理.

密文更新 该运算包括以下两步:

(1) 密钥转换: 计算 $c_1 \leftarrow \mathrm{SwitchKey}(\tau_{s'_j\to s_{j-1}}, c)$, 即将密文 c 转化为模数为 q_j、密钥为 s_{j-1} 下的密文.

(2) 模数转换: 计算 $c_2 \leftarrow \mathrm{Scale}(c_1, q_j, q_{j-1}, 2)$, 即将 c_1 转化为模数为 q_{j-1}、密钥为 s_{j-1} 的密文.

通过密钥转换, 可以将同态乘法会后密文的维数由 $(n+1)^2$ 转换为 $(n+1)$; 通过模数转换, 密文中噪声降低到大约转换前的 q_{j-1}/q_j 倍, 因此在同态乘法后执行 FHE.Refresh 运算, 可以保证后续的同态运算可以继续下去.

体制的安全性是基于格上 LWE 问题难解性假设. 从用户公钥 $A_j (j \in [0, L]\})$ 的生成算法来看, A_j 可看成 N 个 $A_{s,\chi}$ 中元素, 根据 LWE 问题难解性假设, A_j 可看成是从 $\mathbb{Z}_q^{N\times(n+1)}$ 上随机均匀选取的, 因此将不能从密文中得到明文的任何信息,

从而说明体制是安全的. 实际上, Brakerski 等基于 LWE 问题难解性, 给出了对该算法严格的安全性证明 (见文献 [60]).

习　题

习题 13.1　令 L 是 $\mathbb{R}^m$ 的一个加法子群, 证明:

(1) L 是格当且仅当存在 $r > 0$ 使得 $\mathrm{B}(0, r) \cap L = \{0\}$;

(2) 格 L 的任意一个加法子群 L' 仍然构成格.

习题 13.2　对于任给的两个正整数 a 和 b, $\mathbb{Z}a + \mathbb{Z}b$, 集合 $\mathbb{Z}a + \mathbb{Z}b$ 构成格, 但集合 $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ 不构成格.

习题 13.3　证明: 两组格基 $B, B' \in \mathbb{R}^{m\times n}$ 等价, 当且仅当存在一个幺模矩阵 $U \in \mathbb{Z}^{n\times n}$, 使得 $B' = BU$.

习题 13.4　证明: 任意格基所对应的格拉姆矩阵一定是正定的.

习题 13.5　证明: 令 $b_1, \cdots, b_n$ 是欧几里得空间 $\mathbb{R}^m$ 的一组线性无关向量, 归纳定义

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

其中 $\mu_{i,j} = b_i \cdot b_j^*, / b_j^* \cdot b_j^* \ \ (1 \leqslant j < i \leqslant n)$. 那么 $\{b_i^*\}_{1\leqslant i\leqslant n}$ 生成 $\mathbb{R}^m$ 的一组正交向量, 且

$$\sum_{j=1}^{i-1} \mathbb{R} b_j = \sum_{j=1}^{i-1} \mathbb{R} b_j^* \ \ (2 \leqslant i \leqslant n).$$

特别地, 格 $L = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$ 的判别式

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\|, \qquad \det(L) \leqslant \prod_{i=1}^{n} \|b_i\|.$$

习题 13.6　对于格 L 的一组基 $\{\alpha_1, \cdots, \alpha_n\}$, 定义

$$\Pi(\alpha_1, \cdots, \alpha_n) = \left\{ \sum_{i=1}^{n} a_i \alpha_i \,\middle|\, 0 \leqslant a_i < 1 \right\}$$

是 $\mathbb{R}^n$ 中的一个平行多面体, 用 μ 表示 $\mathbb{R}^n$ 上的 Lebesgue 测度, 证明:$\Pi(\alpha_1, \cdots, \alpha_n)$ 的 “ 体积”$\mu(\Pi(\alpha_1, \cdots, \alpha_n)) = \det(L)$.

习题 13.7　证明: 对于给定的背包问题 $P(a_1, \cdots, a_n, s)$, 若背包密度 $d = \dfrac{n}{\max\limits_{1\leqslant i\leqslant n} \{\log_2 a_i\}} > 1$ 时, 背包问题 $P(a_1, \cdots, a_n, s)$ 的解是不唯一的.

附录　一些常用算法

A.1　不可约多项式的判别

假设已经熟知有限域 F_q 的基本理论和多项式环 $F_q[x]$ 上的一些基本算法 (类似于 $\mathbb{Z}$ 上的算法), 如欧几里得算法、最大公因子算法、Legendre 符号算法等. 在构造 F_q 上的 m 次扩张 F_{q^m} 时, 需要寻找 $F_q[x]$ 中一个首一 m 次不可约多项式, 目前一般有两种算法, 一种是确定性 (构造性) 的算法, 在技术上比较复杂, 而第二类概率性算法常被采用, 即对于随机给出一个 m 次首一多项式, 判别其是否是不可约多项式, 重复此过程一直到给出肯定性判断为止, 这便涉及算法成功的可能性有多大.

设 $A_{m,q}$ 为 $F_q[x]$ 中的 m 次首一不可约多项式的个数, 已知

$$A_{m,q} = \frac{1}{m}\sum_{d|m}\mu(d)q^{\frac{m}{d}},$$

那么, $A_{m,q} \sim \dfrac{1}{m}q^m$, $m \to \infty$, 而 q^m 为 m 次首一多项式的总数. 故当 m 充分大时, 随机选择一个 m 次首一多项式是不可约多项式的概率大致为 $\dfrac{1}{m}$.

算法 1.1　不可约多项式的判别

输入:$f(x) \in F_q[x]$, p, r 使 $q = p^r$

输出:Yes 或 No

1. $d \leftarrow \deg f(x)$
2. $u(x) \leftarrow x$
3. For i from 1 to $\left[\dfrac{d}{2}\right]$ 执行

   3.1 for j from 1 to i 执行

   　　$u(x) \leftarrow u(x)^p (\mathrm{mod}\, f(x))$

   　　$j \leftarrow j+1$

   3.2 $\varphi(x) \leftarrow \gcd(u(x)-x, f(x))$

   3.3 if $\varphi(x) \neq 1$ then 返回 “No” and stop
4. 返回 “Yes”

该算法的正确性是由于若 $f(x)$ 可约, 当且仅当存在一个次数为 $i \leqslant \left[\dfrac{\deg f(x)}{2}\right]$ 的不可约多项式 $g(x)$ 作为其因子, 而此时 $\gcd(x^{q^i}-x, f(x)) \neq 1$.

A.2　有限域中平方根的求解

对 F_q^*(q 是奇数) 中的一个元素, 判别其是否是平方元素, 有类似于 $\mathbb{Z}_p^*$ 中的 Legendre 符号算法, 称作多项式 Legendre 符号算法, 可参见文献 [9]. 当知道 $a \in F_q^*$ 是平方元时, 如何来求 a 的平方根呢?

设 $q-1=2^s \cdot t$, t 是奇数, 对 $G=F_q^*$, 它有如下的子群链:

$$H=G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{s-1} \subseteq G_s = G,$$

其中 H 是阶为 t 的子群; 且 $|G_i/G_{i-1}|=2$, 事实上, 若选 α 是 F_q^* 的本原元:$H=\langle\alpha^{2^s}\rangle$, 那么 $G_i=\langle\alpha^{2^{s-i}}\rangle$, $0 \leqslant i \leqslant s$. 因为对 G 中任意非平方元 β, $\beta^{2^{s-i}} \in G_i/G_{i-1}$, 且 $\{1, \beta, \cdots, \beta^{2^s-1}\}$ 是 G/H 的一个陪集代表元系. 因此, G 中任意一个元素 a 一定有唯一的表示

$$a=\beta^e \cdot r, \quad 0 \leqslant e \leqslant 2^s-1, \quad r \in H.$$

求 a 的平方根, 只需分别求 β^i 和 r 的平方根.

β 的选择有 1/2 成功概率. 故求 a 的上述表示, 归结为求 e, 即求 e 的二进制表示 $e=e_0+2e_1+\cdots+2^{s-1}e_{s-1}(e_i \in \{0,1\})$ 的各个分位, 记住 $\{1, \beta^{2^{s-i}}\}$ 是 G_i/G_{i-1} 的一个陪集.

因为 a 是平方元, 且 $a\beta^{-e} \in H$, 取 $e_0=0$, $a\beta^{-e_0} \in G_{s-1}$,

$$e_1=\begin{cases} 0, & a\beta^{-e_0} \in G_{s-2}, \\ 1, & a\beta^{-e_0} \notin G_{s-2}, \end{cases}$$

因为 $\{1, \beta^2\}$ 是 $\dfrac{G_{s-1}}{G_{s-2}}$ 的一个陪集, 故 $a\beta^{-(e_0+2e_1)} \in G_{s-2}$, 按上述思想一直递归下去, 假设知道 $e_0+e_1 2+\cdots+e_{i-1}2^{i-1}$, $1 \leqslant i \leqslant s-1$, 满足

$$a\beta^{-(e_0+\cdots+e_{i-1}2^{i-1})} \in G_{s-i},$$

那么

$$e_i=\begin{cases} 0, & a\beta^{-(e_0+\cdots+e_{i-1}2^{i-1})} \in G_{s-(i+1)}, \\ 1, & a\beta^{-(e_0+\cdots+e_{i-1}2^{i-1})} \notin G_{s-(i+1)}. \end{cases}$$

又因为 $\{1, \beta^{2^i}\}$ 是 $G_{s-i}/G_{s-(i+1)}$ 的一个陪集, 故

$$a\beta^{-(e_0+\cdots+e_i 2^i)} \in G_{s-(i+1)}.$$

当 $i=s-1$ 时, $e=e_0+\cdots+e_{s-1}\cdot 2^{s-1}$, 且 $h=a\beta^{-e}\in G_0=H$. 而 h 是奇数阶元, 显然 $h^{\frac{t+1}{2}}$ 是 h 的平方根, 故

$$\beta^{e_1+\cdots+e_{s-1}\cdot 2^{s-2}}\cdot h^{\frac{t+1}{2}}$$

是 a 的平方根. 综上所述, 有如下算法.

算法 1.2　求 F_q 中平方根

输入:F_q, q 是奇素数的方幂, a 是 F_q 中的平方元

输出:$\sqrt{a}$

1. 随机选取 $\beta\in F_q^*$
2. 若 β 是平方根元 goto 1
3. 分解 $q-1=2^s\cdot t$, t 是奇数
4. $e\leftarrow 0$
5. for $i=1$ to $s-1$ 执行
   5.1 if $(a\beta^{-e})^{2^{s-(i+1)}t}\neq 1$ then $e\leftarrow e+2^i$
6. $h\leftarrow a\beta^{-e}$, $b\leftarrow \beta^{\frac{e}{2}}h^{\frac{t+1}{2}}$
7. 返回 b

A.3　有限域上的分解

设 $q=p^e$, p 素数, $g(x)\in F_q[x]$ 是一个待分解的多项式, $g'(x)$ 是对 $g(x)$ 的求导. 事实上, 若 $g'(x)=0$, 那么 $g(x)$ 是某个多项式的 p 次幂 (习题 1); 若 $g'(x)\neq 0$, 那么 $g(x)/\gcd(g'(x),g(x))$ 无平方因子 (习题 2). 因而有如下算法.

算法 1.3　Squarefree $(g(x))$

输入:$g(x)$

输出:$\{(g_i\ e_i)\}$, g_i 无平方因子, 且 $g=\prod\limits_i g_i^{e_i}$

1. 若 $g'(x)=0$, 求 h 使得 $g=h^p$
   $\{(h_1\ e_1),\cdots,(h_s\ e_s)\}\leftarrow \text{Squarefree}(h)$
   返回 $\{(h_1\ pe_1),\cdots,(h_s\ pe_s)\}$
2. $d\leftarrow \gcd(g,g')$
3. 若 $d=1$, 返回 $\{(g\ 1)\}$
4. 返回 $\{\text{Squarefree}(d),\text{Squarefree}(g/d)\}$

因此可以假设 $g(x)$ 无平方因子, 且 $g(0)\neq 0$, 容易看出, 用下面算法可以

将 $g(x)$ 分解成

$$g(x)=\prod_{i=1}^{\deg(g)} h_i(x),$$

其中 $h_i(x)$ 是 $g(x)$ 的所有 i 次不可约因子的乘积.

算法 1.4

输入:$g(x)$ 首一无平方因子多项式, 且 $g(0)\neq 0$

输出:$h_i(x)(1\leqslant i\leqslant \deg(g))$, 使得 $h_i(x)$ 是 $g(x)$ 的所有 i 次不可约因子的乘积

1. (初始)$h_i\leftarrow 1$ $(1\leqslant i\leqslant \deg(g))$, $h\leftarrow f$, $i\leftarrow 1$
2. $h_i\leftarrow \gcd(h, x^{q^i-1}-1)$, $h\leftarrow h/h_i$
   若 $h=1$, 算法终止, 否则, goto 3
3. $i\leftarrow i+1$
   若 $2i<\deg(h)$, goto 2 , 否则, $h_{\deg(h)}\leftarrow h$, 算法终止

下面对 $g(x)$ 附加个更强的条件, 即 $g(x)=f_1(x)\cdots f_r(x)$, $r\geqslant 2$, f_i 是不可约多项式, $f_i\neq f_j(i\neq j)$, 且 $\deg f_i=\deg f_j=d$, 因此 $\deg g(x)=d\cdot r$, 由中国剩余定理可知

$$R=F[x]/\big(g(x)\big)\cong \frac{F[x]}{\big(f_1(x)\big)}\oplus\cdots\oplus\frac{F[x]}{\big(f_r(x)\big)}\ .$$

以后可将 R 中的元素 a 用坐标 $(a_1,\cdots,a_r)$ 表示, 其中 $a_i\equiv a(\bmod\ f_i)$ $(1\leqslant i\leqslant r)$, 将 R 看成 F_q-线性空间, 令 $B=\{a\in R|\ a^q=a\}$ 是 R 的一个子空间, 可以用 a 的坐标来刻画 B 中的元素.

定理 A.1 $a=(a_1,\cdots,a_r)\in B$ 当且仅当 $a_i\in F_q$, $1\leqslant i\leqslant r$.

证明 因为 $a^q=(a_1^q,\cdots,a_r^q)$, 若 $a_i\in F_q$, 则显然 $a^q=a$, 即 $a\in B$. 反之若 $a^q=a$, 那么 $a_i^q=a_i$, $a_i\in\dfrac{F_q[x]}{(f_i)}\cong F_{q^d}$, 故 a_i 在子域 F_q 中, 证毕.

定义 τ 为 $R\longrightarrow R(a\longmapsto a^q)$ 的 Frobenius 线性映射, 由上述定理可知 $B=\ker(\tau-1)$, 用解 F_q 上的线性方程组的算法就可获得 B 的一组基 $e_1,\cdots,e_r$, 那么 B 中任一个元素均有形式

$$a=\sum_{i=1}^{r}a_ie_i,\quad a_i\in F_q,$$

且 a 是 R 中的可逆元当且仅当 $a_i\neq 0$, $1\leqslant i\leqslant r$, 故 B 中可逆元的个数为 $(q-1)^r$.

情形 1 q 是奇数. 令 a 是 B 中随机选取的一个元素, 若 a 不是可逆元, 且 $a\neq 0$, 那么计算 $\gcd(a,f)$ 便得到 f 的一个真因子, 而 $a=0$ 的概率为 $\dfrac{1}{q^r-(q-1)^r}<$

$\frac{1}{(q-1)^{r-1}} \leqslant \frac{1}{2^{r-1}}$; 若 a 是可逆元, 且 $a \neq \pm 1$, 计算 $s = a^{\frac{q-1}{2}} = (\pm 1, \cdots, \pm 1)$, 那么计算 $\gcd(s-1, f)$, 便得到 f 的一个真因子. 由 a 的随机性可知 s 取 ± 1 也是随机的, 故 $s = \pm 1$ 的概率为 $2/2^r = \frac{1}{2^{r-1}}$.

综合上述, 便可以得一个概率算法, 且出错的概率 $\leqslant \frac{1}{2^{r-1}}$.

算法 1.5

输入:$g(x) \in F_q[x]$ 是若干个相同次数的不可约多项式的乘积

输出:$g(x)$ 的一个真因子

1. 求 $\ker(\tau - 1)$ 的一组基 $e_1, \cdots, e_r$
2. 随机选取 $a_1, \cdots, a_r \in F_q$

   $a \leftarrow \sum_{i=1}^{r} a_i e_i$

   $d(x) \leftarrow \gcd(a, g)$
3. 若 $0 < \deg d(x) < \deg g(x)$, 返回 $d(x)$
4. $s \leftarrow a^{\frac{q-1}{2}}$

   $d(x) \leftarrow \gcd(s-1, g)$　goto 3

为了保证此算法出错的可能性尽可能小, 可以重复上述过程多次.

情形 2　q 是偶数, 可以得到类似的结论 (习题 3).

A.4　Hensel 引理

Hensel 方法的思想是将一些 mod p 下 (即在域 F_p 中) 的结论提升到 modp^e 下 (即在环 $\mathbb{Z}/(p^e)$ 中). 例如, $f(x) \in \mathbb{Z}[x]$, 且已知 $a_0, 0 \leqslant a_0 \leqslant p-1$ 是 $f(x) (\bmod\ p)$ 的单根, 即 $f(a_0) \equiv 0 (\bmod\ p)$ 且 $f'(a_0) \not\equiv 0 (\bmod\ p)$. 如果寻找 $f(x) (\bmod\ p^e)$ 中的一个根且 mod p 下等于 a_0, 用多项式的 Taylor 展开

$$f(x+y) = f(x) + f'(x)y + \frac{f''(x)}{2}y^2 + \cdots,$$

设要求的根为 $a_0 + a_1 p + \cdots + a_{e-1}p^{e-1}$　$(0 \leqslant a_i \leqslant p-1, 1 \leqslant i \leqslant e-1)$, 那么

$$f(a_0 + a_1 p) \equiv f(a_0) + f'(a_0)a_1 p \ (\bmod\ p^2),$$

求得 $a_1 = -\frac{f(a_0)/p}{f'(a_0)} (\bmod\ p)$. 重复上述过程即可求出 $a_2, \cdots, a_{e-1}$, 写出具体算法 (习题 4).

Hensel 方法还能用于求多项式的分解, 用算法的形式来描述它.

算法 1.6

输入:首一 $f \in \mathbb{Z}[x]$, p 素数, e 正整数, 首一多项式 $\bar{g}, \bar{h} \in F_p[x]$ 使得 $f \equiv \bar{g} \cdot \bar{h} (\text{mod } p)$, 且 $\gcd(\bar{g}, \bar{h}) = 1$

输出:首一多项式 $g, h \in \mathbb{Z}_{p^e}[x]$ 使得 $f \equiv g \cdot h (\text{mod } p^e)$ 且 $g \equiv \bar{g} (\text{mod } p)$, $h \equiv \bar{h} (\text{mod } p)$

1. 用广义欧几里得算法求出 $\lambda, \mu \in F_p[x]$ 使得

$$\lambda \bar{g} + \mu \bar{h} = 1, \quad \deg \lambda < \deg \bar{h}, \quad \deg \mu < \deg \bar{g}$$

2. $g \leftarrow \bar{g}$, $h \leftarrow \bar{h}$
3. For $i = 2$ to e do {寻找 mod p^i 的分解}
   3.1 $q \leftarrow \left(\dfrac{f - gh}{p^{i-1}}\right) (\text{mod } p)$
   3.2 $u \leftarrow q\mu (\text{mod } g)$
   3.3 $v \leftarrow q\lambda (\text{mod } h)$
   3.4 $g \leftarrow g + p^{i-1} u$
   3.5 $h \leftarrow h + p^{i-1} v$
4. 返回 (g, h)

算法的正确性证明: 由递归假设 $f \equiv gh\, (\text{mod } p^{i-1})$, 所以 $\left(\dfrac{f - gh}{p^{i-1}}\right)$ 有意义, 又因 f, g, h 均为首一多项式, 所以 $\deg q < \deg f$, 而在 $F_p[x]$ 中有

$$uh + vg = q, \quad \deg(uh + vg) = \deg(q) < \deg f,$$

因此

$$(g + p^{i-1}u)(h + p^{i-1}v) = gh + p^{i-1}(uh + vg) \ \ (\text{mod} p^i) = gh + p^{i-1} \cdot q \equiv f,$$

证毕.

A.5 $\mathbb{Z}[x]$ 中多项式的分解

令 $g(x) \in \mathbb{Z}[x]$ 是整系数、无平方因子、首一的本原 (系数互素) 多项式, $d(g)$ 是其判别式, 选取素数 $p \nmid d(g)$ ($p | d(g)$ 当且仅当 $g(x) (\text{mod } p)$ 有重根), 用 A.3 节 $\bar{g}(x) (\text{mod } p)$ 的分解算法, 求得一个首一因子 $\bar{h}(x)$, 再用 Hensel 引理, 将 $\bar{h}(x)$ 提升到 $g(x)$ 在 $\mathbb{Z}/(p^k)[x]$ 中的一个首一因子 $h(x)$, 使得 $h(x)\ (\text{mod } p) = \bar{h}(x)$, 允许 k 充分大, 由此去判别 $g(x)$ 在 $\mathbb{Z}[x]$ 中是否有不可约因子 $h_0(x)$, 使得 $h_0(x)\ (\text{mod } p) = \bar{h}(x)$, 在肯定的条件下进一步去构造此因子.

令 $l=\deg(h)$, $m=\deg(g)$, 对每个 $l_0\in N$, $l\leqslant l_0\leqslant m$, 选择 k 充分大使得

$$p^{kl}>2^{l_0 m/2}\binom{2l_0}{m}^{m/2}\|g\|^{l_0+m},$$

其中 $\|g\|=\sqrt{g_0^2+g_1^2+\cdots+g_m^2}$, $g(x)=\sum\limits_{i=0}^{m}g_ix^i$. 令

$$L=\left\{u(x)\in\mathbb{Z}[x]|\ \deg u(x)\leqslant l_0,\ h(x)|u(x)(\bmod p^k\mathbb{Z}[x])\right\}$$

定义单射:

$$\varphi:\qquad L\longrightarrow\mathbb{Z}^{l_0+1}$$

$$\sum_{i=0}^{l_0}u_ix^i\longmapsto(u_0,\cdots,u_{l_0})^t\quad,$$

显然 $\varphi(L)$ 是一个整格 (即存在一组基, 基中的每个向量的分量均是整数), 且

$$\varphi\left(\{p^kx^i|\ 0\leqslant i\leqslant l-1\}\cup\{h(x)x^j|\ 0\leqslant j\leqslant l_0-l\}\right)$$

是 $\varphi(L)$ 的一组基, 因此判别式 $d(\varphi(L))=p^{kl}$. 用格基约化算法, 获得 $\varphi(L)$ 的一组 L^3-约化基 $\omega_1,\cdots,\omega_{l_0+1}$.

引理 A.1　设 $g(x)$ 在 $\mathbb{Z}[x]$ 有一因子 $h_0(t)$, $\deg h_0\leqslant l_0$, 且 $\bar{h}(x)|\bar{h}_0(x)$ 当且仅当

$$\|\omega_1\|<\left(p^{kl}/\|g\|^{l_0}\right)^{\frac{1}{m}}.$$

进一步地, 在上述条件成立时, 令 $t=\max\left\{i\mid 1\leqslant i\leqslant l_0+1,\|\omega_i\|<\left(p^{kl}/\|g\|^{l_0}\right)^{\frac{1}{m}}\right\}$, 那么

$$h_0(t)=\gcd(\varphi^{-1}(\omega_1),\cdots,\varphi^{-1}(\omega_t)),\quad 且\deg h_0=l_0+1-t.$$

证明　参见文献 [30].

由此可写出求 $g(x)$ 的一个因子的算法 (练习 7).

参 考 文 献

[1] Adelman L M. The function field sieve. Algorithmic Number Theory LNCS877, 1994: 108–121.

[2] Balasubramanian R, Koblitz N. The impobability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. J. of Cryptology, 1998, 11: 141–145.

[3] Berlekamp E R. Algebraic Coding Theory. New York: McGraw Hill, 1978.

[4] Blake I, Seroussi G, Smart N. Elliptic Curves in Cryptography. Cambridge: Cambridge Univ. Press, 1999.

[5] Blum M, Goldwasser S. An Efficient Probalistic Public-key Encryption Scheme that Hides all Partial Information. Berlin: Springer-Verlage, 1985: 289–302.

[6] Buhler J P, Lenstra Jr. H W, Pomerance C. Factoring Integers with the Number Field Sieve. Berlin: Springer-Verlag, 1993.

[7] Canfield E R, Erodös P, Pomerance C. On a problem of Oppenheim concerning factorization numerorum. J. Number Theory, 1983, 17: 1–28.

[8] Cantor D G. Computing in the Jacobian of hyperelliptic curve. Math. of Computation,1987, 48: 95–101.

[9] Cohen H. A Course in Computational Algebraic Number Theory. Berlin: Springer-Verlag, 1993.

[10] Cohen H, Miyaji A, Ono T. Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. Berlin: Springer-Verlag, 1998: 51–56.

[11] Coppersith D. Fast evalution of logarithms in fields of characteristic. IEEE Transactions on Information Theory, 1984, 30: 587–594.

[12] Couveignes J M. Computing a Square Root for the Number Field Sieve. Berlin: Springer-Verlag, 1993, 95–102.

[13] Davis J A, Hddridge D B. Factorization Using the Quadratic Seve Algorithm. New York: Plenum Press, 1984: 103–113.

[14] Diffie W, Hellman M. New directions in cryptography. IEEE Trans. Inform. Theory, 1976, 22: 472–492.

[15] ElGamal T. A subexponential algorithm for computing discrete logarithms over $GF(p^2)$. IEEE Trans. Inform. Theory, 1985, IT31: 473–481.

[16] Frey G, Rück H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. of Computation, 1994, 62: 865–874.

[17] Frey G, Müller M, Rück H. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Trans. Theory, 1999, 45: 1717–1719.

[18] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984, 28: 270–299.

[19] Gordon D. Discrete logarithms in GF(p) using the number field sieve. SIAM J. Discrete Math., 1993, 6: 312–323.

[20] Hartshorne R. Algebraic Geometry. Berlin: Spring-Verlag, 1977.

[21] IEEE P1363/D3 (Draft version 3). Standard specifications for public key cryptography, May 1998.

[22] Hellman M E, Reyneri J M. Fast Computation of Discrete Logarithms in $GF(q)$. New York: Plenum Press, 1983: 3–13.

[23] Katz N M, Magnr B. Arithmetic Moduli of Elliptic Curves. Princeton: Princeton University Press, 1985.

[24] Koblitz N. Hyperelliptic cryptosystems. J. of Cryptology, 1989, 1: 139–150.

[25] Lang S. Introduction to Algebraic Geometry. New York: Interscience, 1958.

[26] Lang S. Algebra Number Theory. Berlin: Springer-Verlag, 1990.

[27] Lanczos C. Solution of systems of linear equations by minimized iterations. J. res. Nat. Bur. Standard, 1952, 49: 33–35.

[28] Lenstra Jr H W. Factoring integers with elliptic curves. Annals of Mathematics, 1987, 126: 649–673.

[29] Lenstra Jr H W. Algorithms in algebraic number theory. Bull. Amer. Math. Soc., 1992, 26: 211–244.

[30] Lenstra A K, Lenstra Jr H W, Lovasz L. Factoring polynomials with rational coefficients. Math. Ann., 1982, 261: 515–534.

[31] Lenstra A K, Lenstra Jr H W, Manasse M S, et al. The Number Field Sieve. Berlin: Springer-Verlag, 1993, 11–42.

[32] Lichtenbaum S. Duality theorems for curves over p-adic fields. Invent. Math., 1969, 7: 120–136.

[33] Lidl R, Niederreiter H. Finite Fields. New York: Addison-Wesley Publishing Company, 1983.

[34] Menezes A T, Okamoto T, Vanstone S A. Reducing elliptic curve logarithms in a finite field. IEEE Trans. Inform. Theory, 1993, 39: 1639–1646.

[35] Peter L. Montgomery, Speeding the Pollard methods of factorization. Preprint, December, 1985.

[36] Montgomery P L. A Block Lanczos Algorithm for Finding Dependencies over $GF(2)$. Berlin: Springer-Verlag, 1995: 106–120.

[37] Morain F, Olivos J. Speeding up the computations on an elliptic curve using addition–subtraction chains. Info. Theory App1., 1990, 24: 531–543.

[38] Morrison A, Brillhart J. A method of factoring and the factorization of F_7. Math. Comp., 1975, 29: 183–205.

[39] Nguyen P. A Montgomery-like Square Root for the Number Field Sieve. Benlin: Springer-Verlag, 1997.

[40] Pohlig S, Hellman M. An improved algorithm for computing logarithm over $GF(p)$ and the cryptographic significance. IEEE Trans. Inform. Theory, 1978, 24: 106–110.

[41] Pohst M. Computational Algebraic Number Theory. Basel: Birkhauser Verlag, 1993.

[42] Pohst M E, Zassenhaus H. Algorithmic Algebraic Number Theory. Cambridge: Cambridge University Press, 1989.

[43] Pollard J M. Monte Carlo methods for index computation (mod p). Math. of Computation, 1978, 32: 918–924.

[44] Pollard J M. The lattice sieve//Lenstra AK, Lenstra HW Jr (eds.).The Development of number field Sieve. Berlin: Springer-Verlag, 1993: 43–49.

[45] Satoh T, Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Comm. Math. Univ. Sancti Pauli, 1998, 47: 81–92.

[46] Schirokauer O. Discrete logarithms and local units. Phil. Trans. R. Soc. Lond, 1993, A345: 409–423.

[47] Schoof R. Nonsingular plane cubic curves over finite fields. J. of Combinatorial Theory, Series A, 1987, 46: 183–211.

[48] Semaev I. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Maht. of Computation, 1998, 67: 353–356.

[49] Silverman J H. The Arithmetic Elliptic Curves. Berlin: Springe-Verlag, 1986.

[50] Smart N P. The discrete logarithm problem of elliptic curves of trace one. Journal of Cryptology, 1999, 12(3): 193–196.

[51] Smart N P. On the performance of hyperelliptic cryptosystems. Eurocrypt'99, LNCS 1592: 165–175.

[52] 祝跃飞, 裴定一. 异常椭圆曲线上的 DLP 的一个算法. 中国科学 (A辑), 2001, 31: 332–336.

[53] 冯克勤. 代数数论. 北京: 科学出版社, 2000.

[54] 华罗庚. 数论导引. 北京: 科学出版社, 1979.

[55] Ajtai M. The shortest vector problem in l_2 is NP-hard for randomized reductions (extended abstract)10-19. Proc. 30th ACM Symp. on Theory of Computing (STOC), ACM, 1998: 10–19.

[56] van Emde Boas P. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report, University of Amsterdam, Department of Mathematics, Netherlands, 1981.Technical Report 8104.

[57] Haviv I, Regev O. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. Proceedings of STOC'07, ACM, 2007: 469–477.

[58] Dinur I, Kindler G, Raz R, Safa S. Approximating CVP to within almost-polynomial factors is NP-hard. Combinatorica, 2003, 23(2): 205–243.

[59] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput., 2007, 37(1): 267–302.

[60] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ICTS, 2012: 309–325.

[61] Regev O. On lattices, learning with errors, random linear codes, and cryptography. J. ACM, 2009, 56(6): 1–40.

[62] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. Advances in Cryptology-EUROCRYPT 2010, 2010: 1-23.

[63] Micciancio D, Goldwasser S. Complexity of Lattice Problems: A Cryptographic Perspective, volume 671 of The Kluwer International Series in Engineering and Computer Science. Boston: Kluwer Academic Publishers, 2002.

[64] Smart N P, Vercauteren F. Fully homomorphic SIMD operations. Cryptology ePrint Archive, Report 2011, 2011: 133.

[65] Rivest R L, Adleman L, Dertouzos M L. On Data Banks and Privacy Homomorphisms. Academic Press, 1978.

[66] Gentry C. Fully homomorphic encryption using ideal lattices. Proceeding of 29th Annual ACM Symposium on the Theory of Computing, 2009.

[67] Gentry C, Halevi S. Implementing Gentry's fully-homomorphic encryption scheme. Advances in Cryptology-Eurocrypt 2011, 2011: 129–148.

[68] Coster M J, Joux A, LaMacchia B A, et al. Improved low-density subset sum algorithms. Computational complexity, 1992, 2(2): 111–128.

[69] Hoffstein J, Pipher J, Silverman J H. An Introduction to Mathematical Cryptography. Berlin: Springer, 2014.

[70] Karu P, Loikkanen J. Practical comparison of fast public-key cryptosystems//Telecommunications Software and Multimedia, Seminar on Network Security. Citeseer, 2001.

[71] Phong Q. Nguyen and Brigitte Vallée. Berlin: Springer, 2009.

[72] Peikert C. Public-key cryptosystems from the worst-case shortest vector problem. Proc. 41st ACM Symp, on Theory of Computing (STOC), 2009: 333–342.

名 词 索 引

《现代数学基础丛书》已出版书目

(按出版时间排序)

1　数理逻辑基础(上册)　1981.1　胡世华　陆钟万　著
2　紧黎曼曲面引论　1981.3　伍鸿熙　吕以辇　陈志华　著
3　组合论(上册)　1981.10　柯　召　魏万迪　著
4　数理统计引论　1981.11　陈希孺　著
5　多元统计分析引论　1982.6　张尧庭　方开泰　著
6　概率论基础　1982.8　严士健　王隽骧　刘秀芳　著
7　数理逻辑基础(下册)　1982. 8　胡世华　陆钟万　著
8　有限群构造(上册)　1982.11　张远达　著
9　有限群构造(下册)　1982.12　张远达　著
10　环与代数　1983.3　刘绍学　著
11　测度论基础　1983.9　朱成熹　著
12　分析概率论　1984.4　胡迪鹤　著
13　巴拿赫空间引论　1984.8　定光桂　著
14　微分方程定性理论　1985.5　张芷芬　丁同仁　黄文灶　董镇喜　著
15　傅里叶积分算子理论及其应用　1985.9　仇庆久等　编
16　辛几何引论　1986.3　J.柯歇尔　邹异明　著
17　概率论基础和随机过程　1986.6　王寿仁　著
18　算子代数　1986.6　李炳仁　著
19　线性偏微分算子引论(上册)　1986.8　齐民友　著
20　实用微分几何引论　1986.11　苏步青等　著
21　微分动力系统原理　1987.2　张筑生　著
22　线性代数群表示导论(上册)　1987.2　曹锡华等　著
23　模型论基础　1987.8　王世强　著
24　递归论　1987.11　莫绍揆　著
25　有限群导引(上册)　1987.12　徐明曜　著
26　组合论(下册)　1987.12　柯　召　魏万迪　著
27　拟共形映射及其在黎曼曲面论中的应用　1988.1　李　忠　著
28　代数体函数与常微分方程　1988.2　何育赞　著
29　同调代数　1988.2　周伯壎　著

30　近代调和分析方法及其应用　1988.6　韩永生　著
31　带有时滞的动力系统的稳定性　1989.10　秦元勋等　编著
32　代数拓扑与示性类　1989.11　马德森著　吴英青　段海鲍译
33　非线性发展方程　1989.12　李大潜　陈韵梅　著
34　反应扩散方程引论　1990.2　叶其孝等　著
35　仿微分算子引论　1990.2　陈恕行等　编
36　公理集合论导引　1991.1　张锦文　著
37　解析数论基础　1991.2　潘承洞等　著
38　拓扑群引论　1991.3　黎景辉　冯绪宁　著
39　二阶椭圆型方程与椭圆型方程组　1991.4　陈亚浙　吴兰成　著
40　黎曼曲面　1991.4　吕以辇　张学莲　著
41　线性偏微分算子引论(下册)　1992.1　齐民友　著
42　复变函数逼近论　1992.3　沈燮昌　著
43　Banach 代数　1992.11　李炳仁　著
44　随机点过程及其应用　1992.12　邓永录等　著
45　丢番图逼近引论　1993.4　朱尧辰等　著
46　线性微分方程的非线性扰动　1994.2　徐登洲　马如云　著
47　广义哈密顿系统理论及其应用　1994.12　李继彬　赵晓华　刘正荣　著
48　线性整数规划的数学基础　1995.2　马仲蕃　著
49　单复变函数论中的几个论题　1995.8　庄圻泰　著
50　复解析动力系统　1995.10　吕以辇　著
51　组合矩阵论　1996.3　柳柏濂　著
52　Banach 空间中的非线性逼近理论　1997.5　徐士英　李　冲　杨文善　著
53　有限典型群子空间轨道生成的格　1997.6　万哲先　霍元极　著
54　实分析导论　1998.2　丁传松等　著
55　对称性分岔理论基础　1998.3　唐　云　著
56　Gel'fond-Baker 方法在丢番图方程中的应用　1998.10　乐茂华　著
57　半群的 S-系理论　1999.2　刘仲奎　著
58　有限群导引(下册)　1999.5　徐明曜等　著
59　随机模型的密度演化方法　1999.6　史定华　著
60　非线性偏微分复方程　1999.6　闻国椿　著
61　复合算子理论　1999.8　徐宪民　著
62　离散鞅及其应用　1999.9　史及民　编著
63　调和分析及其在偏微分方程中的应用　1999.10　苗长兴　著

64 惯性流形与近似惯性流形 2000.1 戴正德 郭柏灵 著
65 数学规划导论 2000.6 徐增堃 著
66 拓扑空间中的反例 2000.6 汪 林 杨富春 编著
67 拓扑空间论 2000.7 高国士 著
68 非经典数理逻辑与近似推理 2000.9 王国俊 著
69 序半群引论 2001.1 谢祥云 著
70 动力系统的定性与分支理论 2001.2 罗定军 张 祥 董梅芳 编著
71 随机分析学基础(第二版) 2001.3 黄志远 著
72 非线性动力系统分析引论 2001.9 盛昭瀚 马军海 著
73 高斯过程的样本轨道性质 2001.11 林正炎 陆传荣 张立新 著
74 数组合地图论 2001.11 刘彦佩 著
75 光滑映射的奇点理论 2002.1 李养成 著
76 动力系统的周期解与分支理论 2002.4 韩茂安 著
77 神经动力学模型方法和应用 2002.4 阮炯 顾凡及 蔡志杰 编著
78 同调论——代数拓扑之一 2002.7 沈信耀 著
79 金兹堡-朗道方程 2002.8 郭柏灵等 著
80 排队论基础 2002.10 孙荣恒 李建平 著
81 算子代数上线性映射引论 2002.12 侯晋川 崔建莲 著
82 微分方法中的变分方法 2003.2 陆文端 著
83 周期小波及其应用 2003.3 彭思龙 李登峰 谌秋辉 著
84 集值分析 2003.8 李 雷 吴从炘 著
85 数理逻辑引论与归结原理 2003.8 王国俊 著
86 强偏差定理与分析方法 2003.8 刘 文 著
87 椭圆与抛物型方程引论 2003.9 伍卓群 尹景学 王春朋 著
88 有限典型群子空间轨道生成的格(第二版) 2003.10 万哲先 霍元极 著
89 调和分析及其在偏微分方程中的应用(第二版) 2004.3 苗长兴 著
90 稳定性和单纯性理论 2004.6 史念东 著
91 发展方程数值计算方法 2004.6 黄明游 编著
92 传染病动力学的数学建模与研究 2004.8 马知恩 周义仓 王稳地 靳 祯 著
93 模李超代数 2004.9 张永正 刘文德 著
94 巴拿赫空间中算子广义逆理论及其应用 2005.1 王玉文 著
95 巴拿赫空间结构和算子理想 2005.3 钟怀杰 著
96 脉冲微分系统引论 2005.3 傅希林 闫宝强 刘衍胜 著
97 代数学中的 Frobenius 结构 2005.7 汪明义 著

98　生存数据统计分析　2005.12　王启华　著
99　数理逻辑引论与归结原理(第二版)　2006.3　王国俊　著
100　数据包络分析　2006.3　魏权龄　著
101　代数群引论　2006.9　黎景辉　陈志杰　赵春来　著
102　矩阵结合方案　2006.9　王仰贤　霍元极　麻常利　著
103　椭圆曲线公钥密码导引　2006.10　祝跃飞　张亚娟　著
104　椭圆与超椭圆曲线公钥密码的理论与实现　2006.12　王学理　裴定一　著
105　散乱数据拟合的模型方法和理论　2007.1　吴宗敏　著
106　非线性演化方程的稳定性与分歧　2007.4　马　天　汪宁宏　著
107　正规族理论及其应用　2007.4　顾永兴　庞学诚　方明亮　著
108　组合网络理论　2007.5　徐俊明　著
109　矩阵的半张量积:理论与应用　2007.5　程代展　齐洪胜　著
110　鞅与 Banach 空间几何学　2007.5　刘培德　著
111　非线性常微分方程边值问题　2007.6　葛渭高　著
112　戴维-斯特瓦尔松方程　2007.5　戴正德　蒋慕蓉　李栋龙　著
113　广义哈密顿系统理论及其应用　2007.7　李继彬　赵晓华　刘正荣　著
114　Adams 谱序列和球面稳定同伦群　2007.7　林金坤　著
115　矩阵理论及其应用　2007.8　陈公宁　著
116　集值随机过程引论　2007.8　张文修　李寿梅　汪振鹏　高　勇　著
117　偏微分方程的调和分析方法　2008.1　苗长兴　张　波　著
118　拓扑动力系统概论　2008.1　叶向东　黄　文　邵　松　著
119　线性微分方程的非线性扰动(第二版)　2008.3　徐登洲　马如云　著
120　数组合地图论(第二版)　2008.3　刘彦佩　著
121　半群的 S-系理论(第二版)　2008.3　刘仲奎　乔虎生　著
122　巴拿赫空间引论(第二版)　2008.4　定光桂　著
123　拓扑空间论(第二版)　2008.4　高国士　著
124　非经典数理逻辑与近似推理(第二版)　2008.5　王国俊　著
125　非参数蒙特卡罗检验及其应用　2008.8　朱力行　许王莉　著
126　Camassa-Holm 方程　2008.8　郭柏灵　田立新　杨灵娥　殷朝阳　著
127　环与代数(第二版)　2009.1　刘绍学　郭晋云　朱　彬　韩　阳　著
128　泛函微分方程的相空间理论及应用　2009.4　王　克　范　猛　著
129　概率论基础(第二版)　2009.8　严士健　王隽骧　刘秀芳　著
130　自相似集的结构　2010.1　周作领　瞿成勤　朱智伟　著
131　现代统计研究基础　2010.3　王启华　史宁中　耿　直　主编

132　图的可嵌入性理论(第二版)　2010.3　刘彦佩　著
133　非线性波动方程的现代方法(第二版)　2010.4　苗长兴　著
134　算子代数与非交换 L_p 空间引论　2010.5　许全华　吐尔德别克　陈泽乾　著
135　非线性椭圆型方程　2010.7　王明新　著
136　流形拓扑学　2010.8　马　天　著
137　局部域上的调和分析与分形分析及其应用　2011.6　苏维宜　著
138　Zakharov 方程及其孤立波解　2011.6　郭柏灵　甘在会　张景军　著
139　反应扩散方程引论(第二版)　2011.9　叶其孝　李正元　王明新　吴雅萍　著
140　代数模型论引论　2011.10　史念东　著
141　拓扑动力系统——从拓扑方法到遍历理论方法　2011.12　周作领　尹建东　许绍元　著
142　Littlewood-Paley 理论及其在流体动力学方程中的应用　2012.3　苗长兴　吴家宏　章志飞　著
143　有约束条件的统计推断及其应用　2012.3　王金德　著
144　混沌、Mel′nikov 方法及新发展　2012.6　李继彬　陈凤娟　著
145　现代统计模型　2012.6　薛留根　著
146　金融数学引论　2012.7　严加安　著
147　零过多数据的统计分析及其应用　2013.1　解锋昌　韦博成　林金官　编著
148　分形分析引论　2013.6　胡家信　著
149　索伯列夫空间导论　2013.8　陈国旺　编著
150　广义估计方程估计方法　2013.8　周　勇　著
151　统计质量控制图理论与方法　2013.8　王兆军　邹长亮　李忠华　著
152　有限群初步　2014.1　徐明曜　著
153　拓扑群引论(第二版)　2014.3　黎景辉　冯绪宁　著
154　现代非参数统计　2015.1　薛留根　著
155　三角范畴与导出范畴　2015.5　章　璞　著
156　线性算子的谱分析(第二版)　2015.6　孙　炯　王　忠　王万义　编著
157　双周期弹性断裂理论　2015.6　李　星　路见可　著
158　电磁流体动力学方程与奇异摄动理论　2015.8　王　术　冯跃红　著
159　算法数论(第二版)　2015.9　裴定一　祝跃飞　编著

(O-6080.31)

www.sciencep.com



科学数理分社
电 话：(010) 64019814
Email：lijingke@mail.sciencep.com

销售分类建议：高等数学

定 价：78.00 元